

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

OSCAR DANIEL BELTRÁN RAMIREZ

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INFORMATICA ECBTI
PROGRAMA EN INGENIERIA DE SISTEMAS
NEIVA
2021

SOLUCIÓN DE DOS ESCENARIOS PRESENTES EN ENTORNOS
CORPORATIVOS BAJO EL USO DE TECNOLOGÍA CISCO

OSCAR DANIEL BELTRAN RAMIREZ

Trabajo final para optar por el título de INGENIERIA DE SISTEMAS

Magister MARIA ALEJANDRA LOPEZ

UNIVERSIDAD ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS TECNOLOGIA E INFORMATICA ECBTI
PROGRAMA EN INGENIERIA DE SISTEMAS

NEIVA

2021

Nota de aceptación:

Firma del presidente del jurado

Firma del jurado

Firma del jurado

NEIVA, 27 de Noviembre de 2021

DEDICATORIA

A mis padres Lía Constanza Ramírez y Fabio Beltrán (Q.E.P.D), mi esposa Lady Johana Rodriguez Trujillo, Mis Hijos Miguel y Diana, los cuales han sido un apoyo para la culminación de este proyecto, me dieron aliento en los momentos en donde creía que no podía alcanzar los objetivos, me animaban a continuar sin importar los obstáculos que se presentaban. Sobre todo, me tuvieron la paciencia que en muchos casos faltaba

AGRADECIMIENTOS

A mi madre y a mi esposa, quienes me animaron con la iniciación de este proyecto, a mis amigos que aportaron con su conocimiento y a Dios por concederme la salud y abrirme la mente en los momentos donde se estancaba la imaginación.

CONTENIDO

GLOSARIO	10
RESUMEN.....	11
ABSTRACT.....	12
INTRODUCCION	13
desarrollo del trabajo final.....	14
1. Desarrollo del primer escenario	14
1.1. Construcción en el simulador de red	14
1.2. Desarrollo del esquema del direccionamiento IP para LAN1 y LAN2.....	15
1.3. Configuración de aspectos básicos de los dispositivos.....	17
2. Desarrollo del segundo escenario	24
2.1. Inicialización de dispositivos.	25
2.2. Configuración de ajustes básicos en dispositivos.	27
2.3. Configuración de seguridad de switches, VLAN y routing entre VLAN. 41	
2.4. Configuración de protocolo de routing dinámico OSPF.....	54
2.5. Implementación de DHCP y NAT para IPv4	58
2.6. Configuración de NTP.....	63
2.7. Configuración y verificación de listas de control de acceso (ACL)	64
CONCLUSIONES	68
BIBLIOGRAFÍA	69

LISTA DE FIGURAS

Figura 1. Topología de red del primer escenario.....	14
Figura 2 Simulación del primer escenario en Packet Tracer.	15
Figura 3 Primera sección de comandos para configuración del router.....	18
Figura 4 Segunda sección de comandos para configuración del router.....	19
Figura 5 Primera sección de comandos para configuración del switch	20
Figura 6 Segunda sección de comandos para configuración del switch	21
Figura 7 Configuraciones de direcciones para el equipo A.	22
Figura 8 Configuraciones de direcciones para el equipo B.	23
Figura 9 Simulación final del primer escenario con conexión entre los equipos A y B.	24
Figura 10 Topología de red del segundo escenario	25
Figura 11 Instrucciones en CLI para la configuración del router R1	29
Figura 12 Instrucciones en CLI para la configuración del router R3.....	34
Figura 13 Instrucciones en CLI para la configuración del switch S1	36
Figura 14 Instrucciones en CLI para la configuración del switch S3	37
Figura 15 Verificación de la conexión de la red entre R1 a R2	39
Figura 16 Verificación de la conexión de la red entre R2 a R3	40
Figura 17 Verificación de la conexión de la red entre PC internet a Gateway predeterminado.....	41
Figura 18 Instrucciones de seguridad en CLI para la configuración del switch S1.	43
Figura 19 Instrucciones de seguridad en CLI para la configuración del switch S3.	45
Figura 20 Instrucciones de seguridad en CLI para la configuración del router R1.	47
Figura 21 Verificación de la conectividad de la red desde S1 a R1 VLAN 99	50
Figura 22 Verificación de la conectividad de la red desde S3 a R1 VLAN 99	51
Figura 23 Verificación de la conectividad de la red desde S3 a R1 VLAN 21	52
Figura 24 Verificación de la conectividad de la red desde S1 a R1 VLAN 21	53
Figura 25 Instrucciones en CLI para configuraciones de protocolo OSPF en R1	53

Figura 26 Instrucciones en CLI para configuraciones de protocolo OSPF en R2...	55
Figura 27 Instrucciones en CLI para configuraciones de protocolo OSPFv3 en R3.	57
Figura 28 Instrucciones en CLI para la configuración de DHCP en R1	60
Figura 29 Instrucciones en CLI para la configuración de NAT estática y dinámica en R2.	61
Figura 30 Instrucciones en CLI para la configuración de NTP.	64
Figura 31 Instrucciones en CLI para la restricción de acceso a líneas vty	65
Figura 32 Simulación final de la topología del segundo escenario.....	67

LISTA DE TABLAS

Tabla 1 Características de la dirección IPv4 para LAN1	16
Tabla 2 Características de la dirección IPv4 para LAN2	16
Tabla 3 Direcciones IP para los dispositivos implícitos en el primer escenario	16
Tabla 4 Instrucciones y comandos respectivos para el reinicio de los dispositivos del segundo escenario.....	26
Tabla 5 Instrucciones y comandos respectivos para el reinicio de los dispositivos del segundo escenario.....	27
Tabla 6 Listado de instrucciones o tareas para la configuración del router R1	28
Tabla 7 Listado de instrucciones o tareas para la configuración del router R2	30
Tabla 8 Listado de instrucciones o tareas para la configuración del router R3	32
Tabla 9 Listado de instrucciones o tareas para la configuración del switch S1	35
Tabla 10 Listado de instrucciones o tareas para la configuración del switch S3....	36
Tabla 11 Resultados de conexión haciendo ping entre los dispositivos configurados.	37
Tabla 12 Listado de instrucciones para configuraciones de seguridad en el switch S1	42
Tabla 13 Listado de instrucciones para configuraciones de seguridad en el switch S3	44
Tabla 14 Listado de instrucciones para configuraciones de seguridad en el router R1.	46
Tabla 15 Resultados de conexión haciendo ping entre los dispositivos configurados para seguridad	48
Tabla 16 Listado de instrucciones para configuraciones de protocolo OSPF en R1.	54
Tabla 17 Listado de instrucciones para configuraciones de protocolo OSPF en R1.	55
Tabla 18 Listado de instrucciones para configuraciones de protocolo OSPFv3 en R3.	56

Tabla 19 Listado de comandos para verificar el funcionamiento del protocolo OSPF.	57
Tabla 20 Listado de instrucciones para la configuración de DHCP en R1	58
Tabla 21 Listado de instrucciones para la configuración de NAT estática y dinámica en R2	60
Tabla 22 Listado de comandos para la verificación del protocolo DHCP y NAT estática y dinámica en R2	62
Tabla 23 Listado de instrucciones para la configuración de NTP	63
Tabla 24 Listado de instrucciones para la configuración de restricción a líneas vty.	64
Tabla 25 Listado de comandos en CLI	66

GLOSARIO

Broadcast: Mensaje que se trasmite a todos los miembros de una red.

CISCO: Empresa desarrolladora de equipos de comunicaciones.

Conectividad: Capacidad de mantener una comunicación o sostener una vinculación en diferentes dispositivos.

DHCP: Protocolo de configuración dinámica donde un servidor asigna dinámicamente una dirección IP.

Dirección IP: Es una dirección que identifica un dispositivo en una red.

DNS: Sistema que ayuda al usuario a conectarse con sitio en internet al hacer la lectura y gestión de los dominios existentes.

IP Estática: Dirección fija de una dirección IP, no cambia el número.

EXEC: Ejecuta un comando.

Gateway: Establecer comunicación entre múltiples entornos.

Gigabyte: unidad de medidas de datos.

Host: Computador o maquina conectada a una red o dominio con un numero de IP definido.

Interconexión: Unión de varias redes o dispositivos.

LAN: Red de área local.

MAC: Dirección física de una tarjeta de red.

NAT: Es un intérprete o traductor de peticiones.

Network: Interconexión de redes.

Programa Packet Tracer: Programas para hacer simulaciones en un entorno de red.

Router: Es un enrutador que permite interconectar computadoras que funcionen en el marco de una red.

RESUMEN

En el siguiente documento se presenta el desarrollo final de trabajo al curso de Diplomado de profundización en CISCO (LAN/WAN) donde a partir del programa de simulación de redes CISCO Packet Tracer se crea un escenario de red pequeña con el fin de evaluar y poner a prueba los conocimientos en redes de área local LAN y WAN, accediendo y modificando los parámetros de red de estas conexiones como direcciones IP, direcciones MAC, ajustes básicos de seguridad, configuraciones de host y verificación de conexión respectivamente.

Palabras clave: CISCO, CCNP, canales, CCNP, Conmutación, Etherchannel, Enrutamiento, router, Electronica, switch, redes y protocolos.

ABSTRACT

The next document presents the final development of work to the course of Diploma of deepening in CISCO (LAN / WAN) where from the cisco packet tracer network simulation program a small network scenario is created in order to evaluate and test the knowledge in local area networks LAN and WAN, accessing and modifying the network parameters of these connections such as IP addresses, MAC addresses, basic security settings, host configurations and connection verification respectively.

Keywords: Switching, Electronics. CCNP, channels, Etherchannel, CISCO, CCNP, Routing, Networks, , switch, router, and protocols.

INTRODUCCION

El uso de redes informáticas esta implícita en nuestra vida diaria, la interconexión que se logra tener gracias a estas tecnologías ha permitido que la sociedad este constantemente comunicada, lo cual causa un efecto de beneficio en todos los ámbitos posibles, ya bien sean sociales, culturales, empresariales, recreativos y así sucesivamente, mas sin embargo el conocimiento y la teoría que esta tras esta tecnología se puede considerar que es muy desconocida.

Los programas de simulación suelen ser una herramienta bastante interactiva con la que usuarios novatos o inexpertos en el campo, tengan un acercamiento al tema y de ser posible despierten un interés sobre este; todo esto es algo que se puede lograr mediante el programa Packet Tracer al ser un software de manejo sencillo y de fácil comprensión, dicho trabajo final que se presenta a continuación pone como ejemplo, un método de conocimiento sobre topología de redes y configuración de las mismas ya bien sea a través de un entorno virtual o mediante programación logrando que el usuario se acomode con el que mejor le parezca y que de esta manera pueda adquirir o empezar una formación en la teoría de redes y transmisión.

Referente al trabajo de investigación, el conocimiento sobre redes de área local, uso de corta fuegos o gestión de servidores y conocer que distintas formas pueden ser trabajados mediante Packet Tracer es un punto vital para las personas inmersas en el tema. Es una forma de identificar y trabajar directamente sobre estos dispositivos sin la necesidad de tenerlos de forma física lo cual puede llegar a ser complicado e incluso también puede llegar a ser como una herramienta de capacitación para un posible futuro desempeño en campo de esta área.

DESARROLLO DEL TRABAJO FINAL

A continuación, se presentan dos escenarios los cuales constan de dos topologías de tipo LAN y de tipo WAN empleando el programa Packet Tracer, en este caso, las simulaciones que se anexan a este documento se encuentran en la versión 8.0.1.0064 de dicho programa.

1. Desarrollo del primer escenario

Para el primer escenario se nos presenta como ya se mencionó, una topología de tipo LAN o red de área local, esto se observa en la figura 1.

Figura 1. Topología de red del primer escenario.



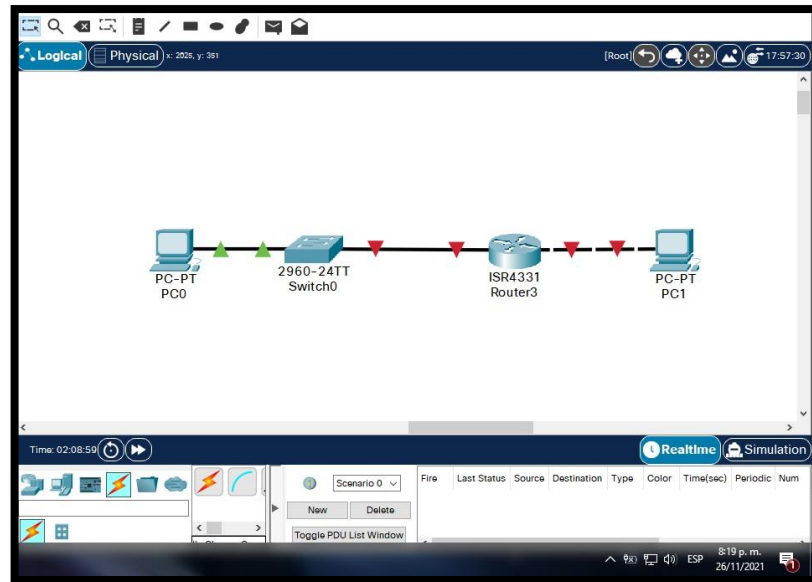
Fuente. (CISCO, 2017)

A partir de esto, se procede a realizar los objetivos propuestos.

1.1. Construcción en el simulador de red.

Con la observación de los elementos requeridos de la figura 1, se estima el uso de dos equipos de cómputo, un switch y un router, la conexión realizada en el programa Packet Tracer se observa a continuación.

Figura 2 Simulación del primer escenario en Packet Tracer.



Fuente. *Propia.*

1.2. Desarrollo del esquema del direccionamiento IP para LAN1 y LAN2.

Para la dirección IPv4 se crean dos subredes con la cantidad de host que son requeridos, en este caso el direccionamiento estará dado por:

- 192.168.8.0/24.
- Host Subred LAN1: 100
- Host Subred LAN2: 50
- Primera dirección de host de la subred LAN1: R1 G0/0/1
- Primera dirección de host de la subred LAN2: R1 G0/0/0
- Ultima dirección de host de la subred LAN1: PC-A
- Ultima dirección de host de la subred LAN2: PC-B

En este caso entonces, el host de LAN1 al necesitar 100, las características serán:

Tabla 1 Características de la dirección IPv4 para LAN1.

Segmentación de IP	192.168.8.0/25.
Rango de hosts	192.168.8.1-192.168.8.126
Total host	126
Broadcast	192.168.8.127

Fuente. *Propia.*

De esta forma aseguramos que haya posibilidad para 100 host y quedan 26 para futuras nuevas conexiones.

Ahora en el caso de LAN2 al necesitar 50 host, las características serán:

Tabla 2 Características de la dirección IPv4 para LAN2.

Segmentación de IP	192.168.8.64/26.
Rango de hosts	192.168.8.129 -192.168.8.190
Total host	64
Broadcast	192.168.8.191

Fuente. *Propia.*

De esta forma aseguramos que haya posibilidad para 50 host

Ya con esto, entonces procedemos a cumplir las especificaciones mencionadas arriba, entonces:

Tabla 3 Direcciones IP para los dispositivos implícitos en el primer escenario.

R1 G0/0/1	192.168.8.1/25
R1 G0/0/0	192.168.8.129/25
PC-A	192.168.8.126/25
PC-B	192.168.8.129/25

Fuente. *Propia.*

A partir de estas direcciones y subfijo de red podemos determinar la mascara de red para cada uno, así como la Gateway necesaria para los equipos de cómputo.

1.3. Configuración de aspectos básicos de los dispositivos.

Ya con las direcciones definidas, se procede a configurar mediante consola tanto el router como el switch, lo cual se observa a continuación.

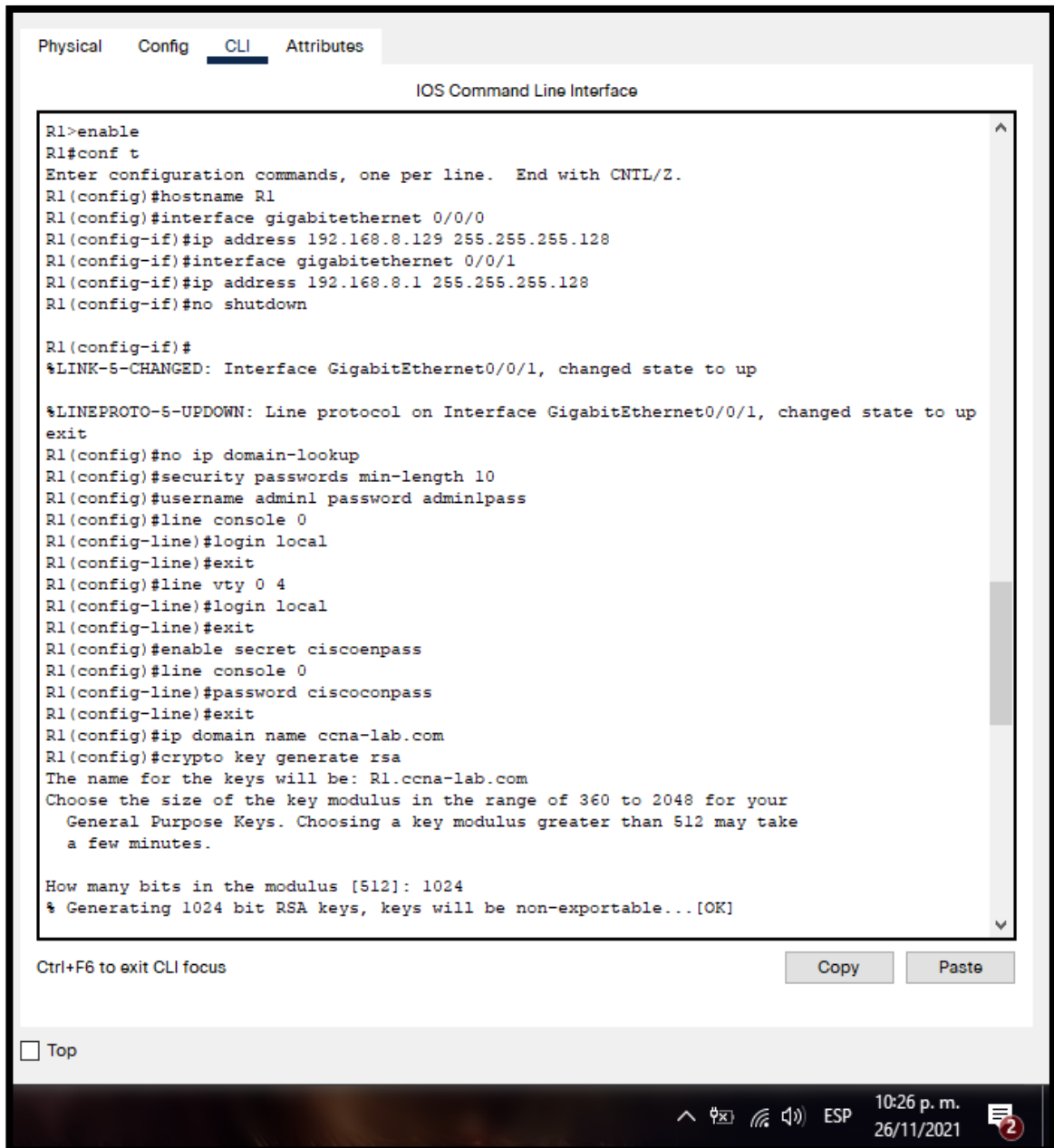
1.3.1. Paso 1: Configuración del router y del switch

Para la configuración del router, la guía especifica los siguientes ítems de configuración mediante una tabla, algunos de estos se listan a continuación.

- Desactivación de DNS.
- Nombre del router: R1
- Nombre de dominio.
- Contraseñas para la consola, de usuario, de privilegio tipo EXEC.
- Configuración de Saludo en pantalla.
- Configuración de las conexiones Gigabyte en el router, descripción de las mismas y establecimiento de IP.

Entre algunos otros, a partir de la GUI que ofrece el programa Packet Tracer, se accede a la terminal de comandos de configuración o CLI, en la cual se ingresan los respectivos comandos para llevar a cabo estas configuraciones requeridas, estos comandos se observan a continuación en la figura 3.

Figura 3 Primera sección de comandos para configuración del router.



```
Physical Config CLI Attributes
IOS Command Line Interface

R1>enable
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#hostname R1
R1(config)#interface gigabitethernet 0/0/0
R1(config-if)#ip address 192.168.8.129 255.255.255.128
R1(config-if)#interface gigabitethernet 0/0/1
R1(config-if)#ip address 192.168.8.1 255.255.255.128
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up
exit
R1(config)#no ip domain-lookup
R1(config)#security passwords min-length 10
R1(config)#username admin1 password admin1pass
R1(config)#line console 0
R1(config-line)#login local
R1(config-line)#exit
R1(config)#line vty 0 4
R1(config-line)#login local
R1(config-line)#exit
R1(config)#enable secret ciscoenpass
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#exit
R1(config)#ip domain name ccna-lab.com
R1(config)#crypto key generate rsa
The name for the keys will be: R1.ccna-lab.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
```

Ctrl+F6 to exit CLI focus

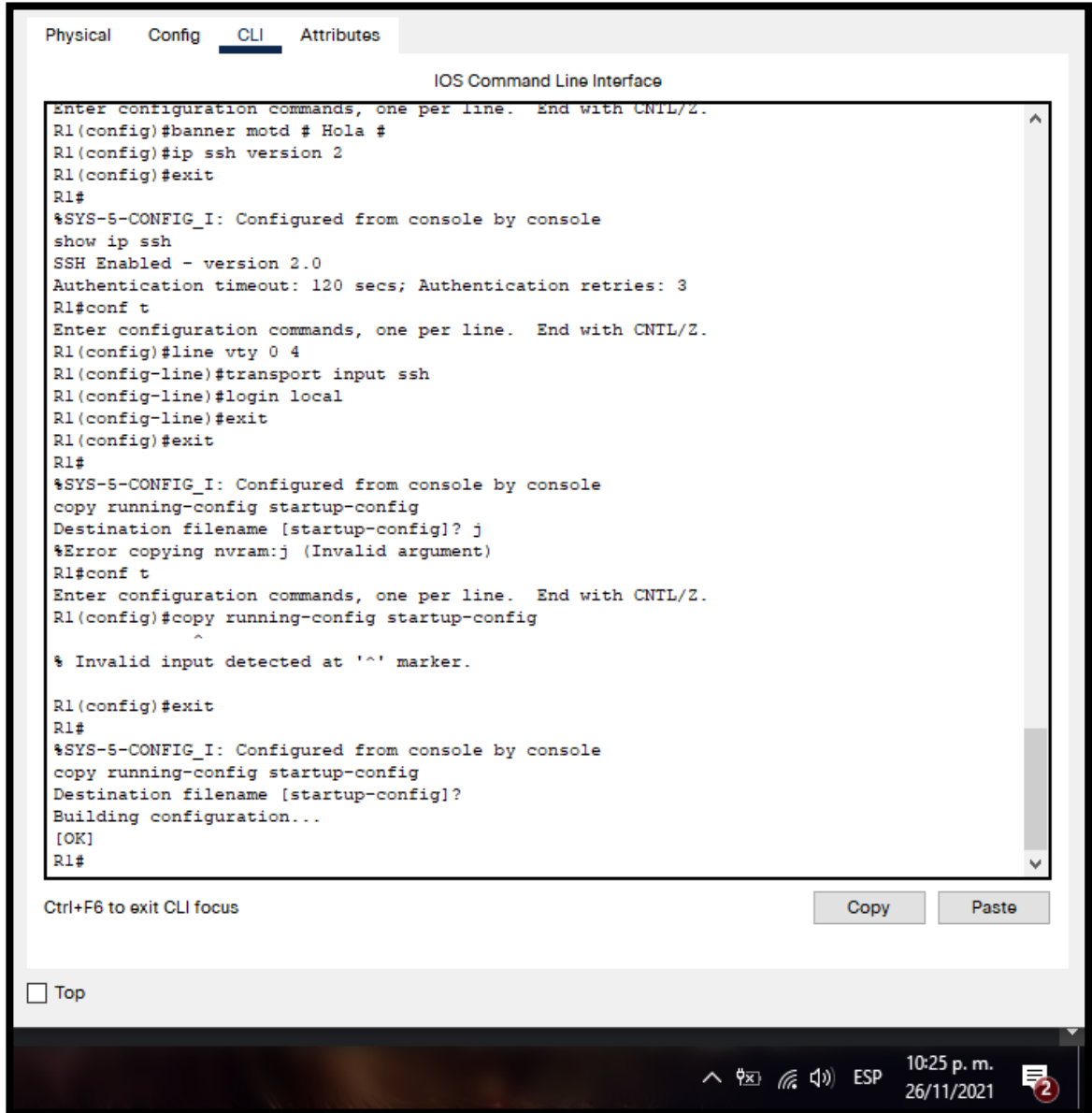
Copy Paste

☐ Top

10:26 p. m.
26/11/2021

Fuente. Propia.

Figura 4 Segunda sección de comandos para configuración del router.



```
Physical  Config  CLI  Attributes

IOS Command Line Interface

Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#banner motd # Hola #
R1(config)#ip ssh version 2
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#line vty 0 4
R1(config-line)#transport input ssh
R1(config-line)#login local
R1(config-line)#exit
R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
copy running-config startup-config
Destination filename [startup-config]? j
%Error copying nvram:j (Invalid argument)
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#copy running-config startup-config
^
% Invalid input detected at '^' marker.

R1(config)#exit
R1#
%SYS-5-CONFIG_I: Configured from console by console
copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

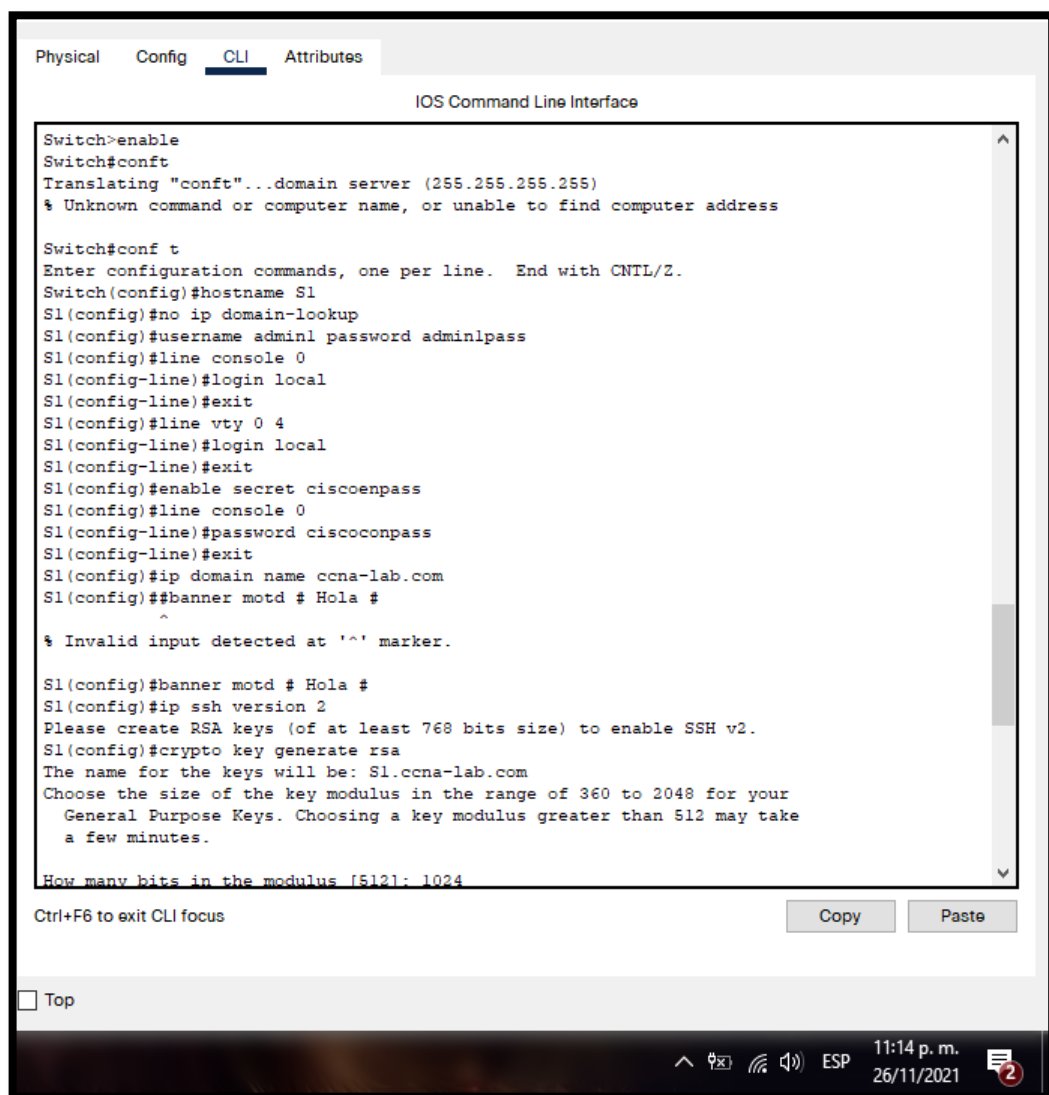
10:25 p.m.
26/11/2021

Fuente. *Propia.*

Con esto, entonces el usuario para ingresar al sistema es: admin1, la contraseña general es: admin1pass, y para acceder al modo privilegiado será el mismo usuario pero la contraseña es: ciscosnas.

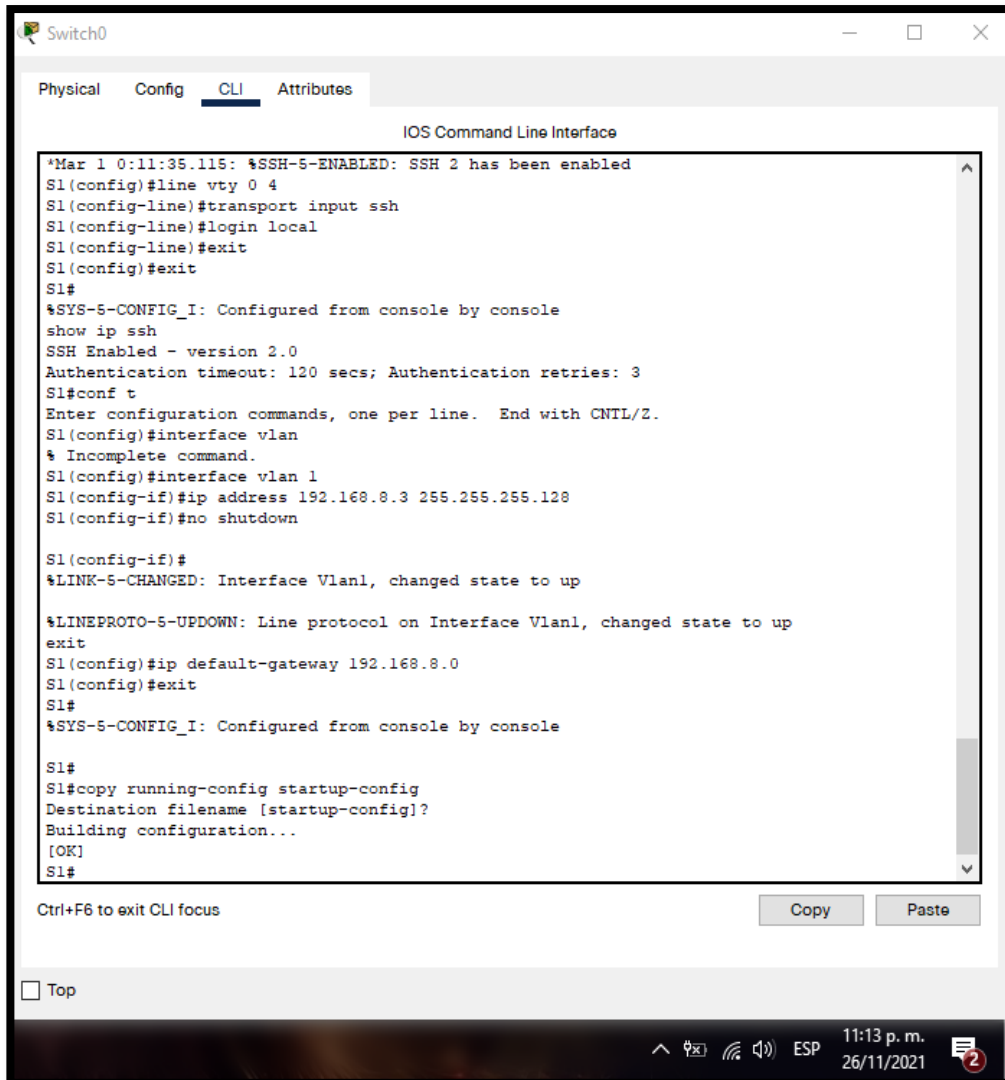
La configuración del switch es muy similar a la del router, las diferencias más notables es una asignación de Gateway y SVI, a continuación, se detallan los comandos empleados.

Figura 5 Primera sección de comandos para configuración del switch.

The image is a screenshot of a network switch's Command Line Interface (CLI) in configuration mode. The window has tabs for 'Physical', 'Config', 'CLI' (which is active), and 'Attributes'. The title bar says 'IOS Command Line Interface'. The CLI shows a sequence of commands being entered to configure a switch named 'S1'. The commands include enabling privileged EXEC mode, entering configuration mode, setting the hostname to 'S1', disabling domain lookup, setting a username 'admin1' with password 'admin1pass', configuring console and vty lines for local login, enabling secret passwords, setting a domain name 'ccna-lab.com', and configuring a MOTD banner. The session ends with the generation of RSA keys for SSH v2, with a key modulus of 1024 bits chosen. The bottom of the window shows a taskbar with system icons, the time '11:14 p. m.', the date '26/11/2021', and a notification icon with the number '2'.

Fuente. *Propia.*

Figura 6 Segunda sección de comandos para configuración del switch.



The screenshot shows a network switch configuration window titled "Switch0". It has tabs for "Physical", "Config", "CLI", and "Attributes", with "CLI" selected. The main area is titled "IOS Command Line Interface" and displays a series of commands and system messages. The commands include enabling SSH, configuring VTY lines, setting the login local, and configuring interface VLAN 1 with an IP address and no shutdown. The system messages indicate that SSH is enabled and the interface state has changed to up. The window also has a "Copy" button and a "Paste" button at the bottom right.

```
*Mar 1 0:11:35.115: %SSH-5-ENABLED: SSH 2 has been enabled
S1(config)#line vty 0 4
S1(config-line)#transport input ssh
S1(config-line)#login local
S1(config-line)#exit
S1(config)#exit
S1#
*SYS-5-CONFIG_I: Configured from console by console
show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
S1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#interface vlan
% Incomplete command.
S1(config)#interface vlan 1
S1(config-if)#ip address 192.168.8.3 255.255.255.128
S1(config-if)#no shutdown

S1(config-if)#
*LINK-5-CHANGED: Interface Vlan1, changed state to up

*LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
exit
S1(config)#ip default-gateway 192.168.8.0
S1(config)#exit
S1#
*SYS-5-CONFIG_I: Configured from console by console

S1#
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
S1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

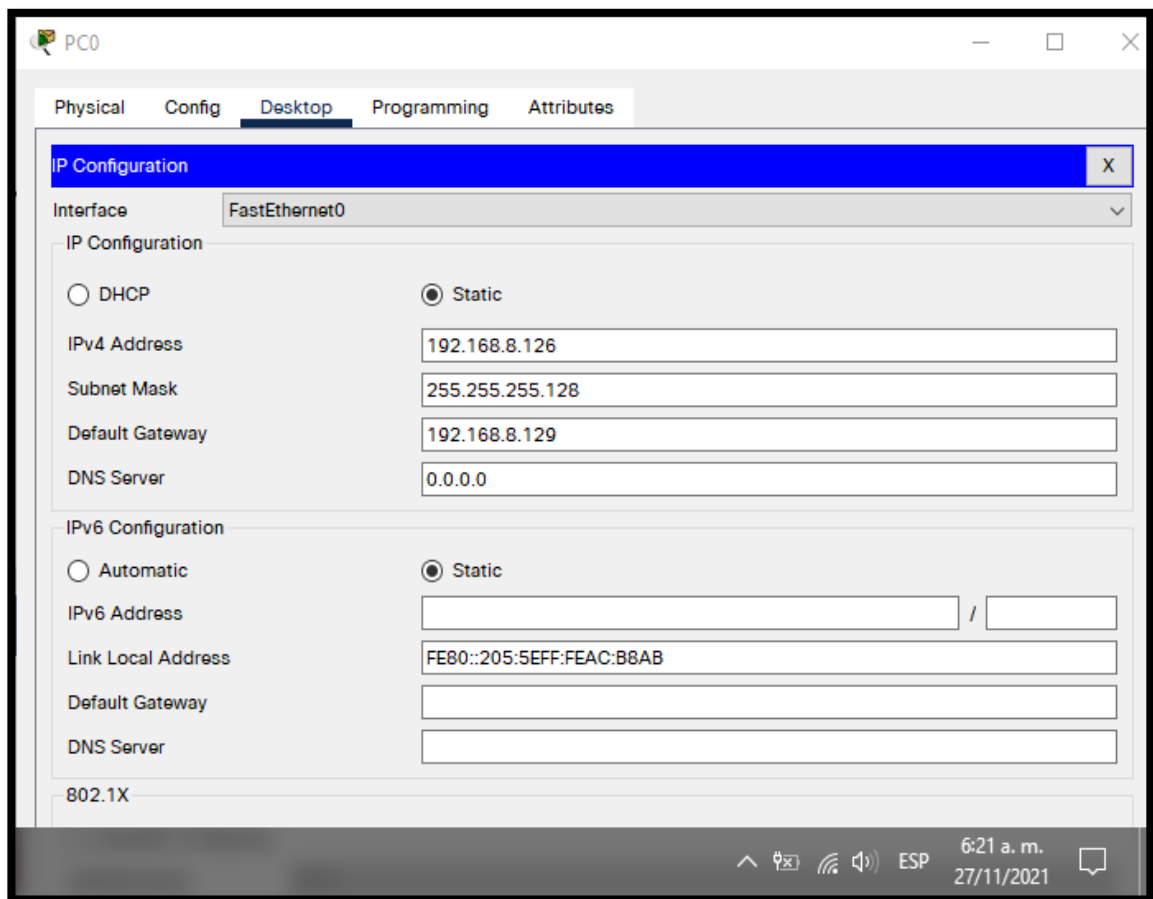
11:13 p. m.
26/11/2021

Fuente. *Propia.*

1.3.2. Paso 2: Configuración de los equipos.

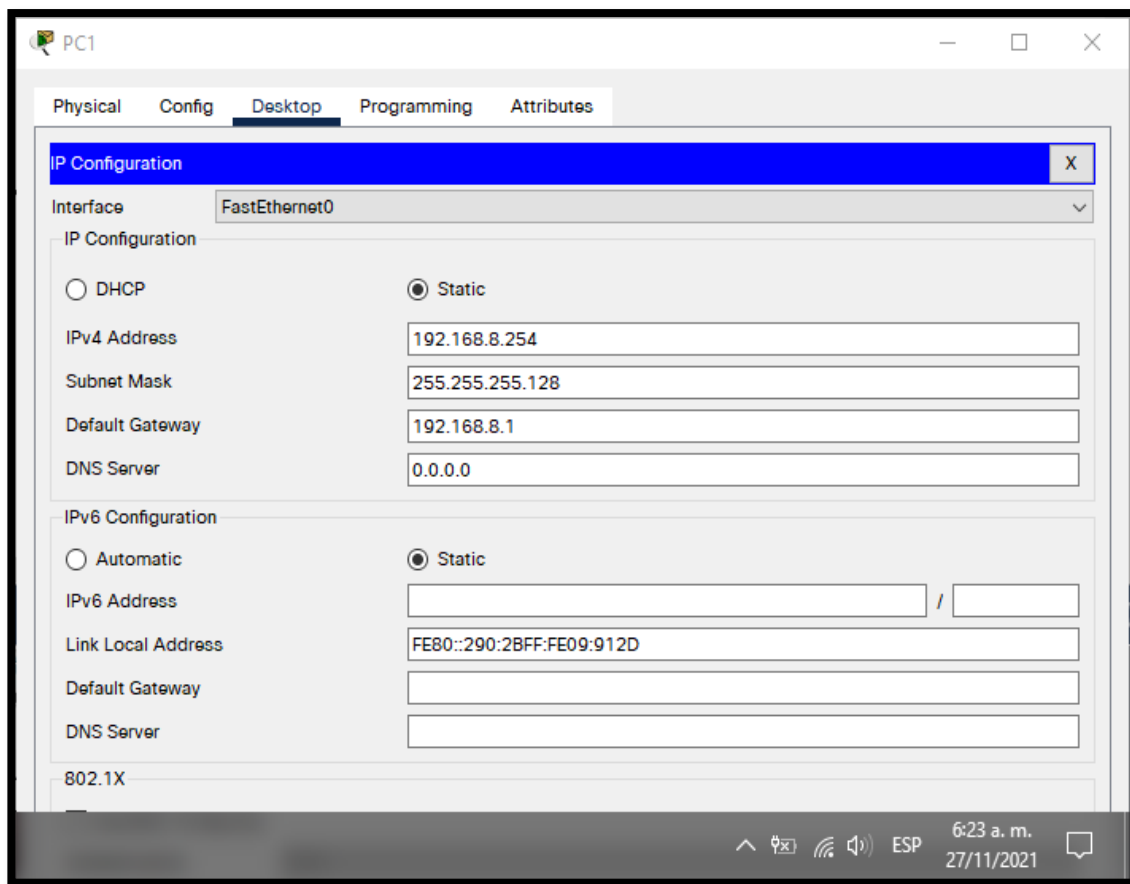
Por ultimo se realiza la configuración de ip para los equipos de cómputo, esto se observa a continuación.

Figura 7 Configuraciones de direcciones para el equipo A.



Fuente. *Propia.*

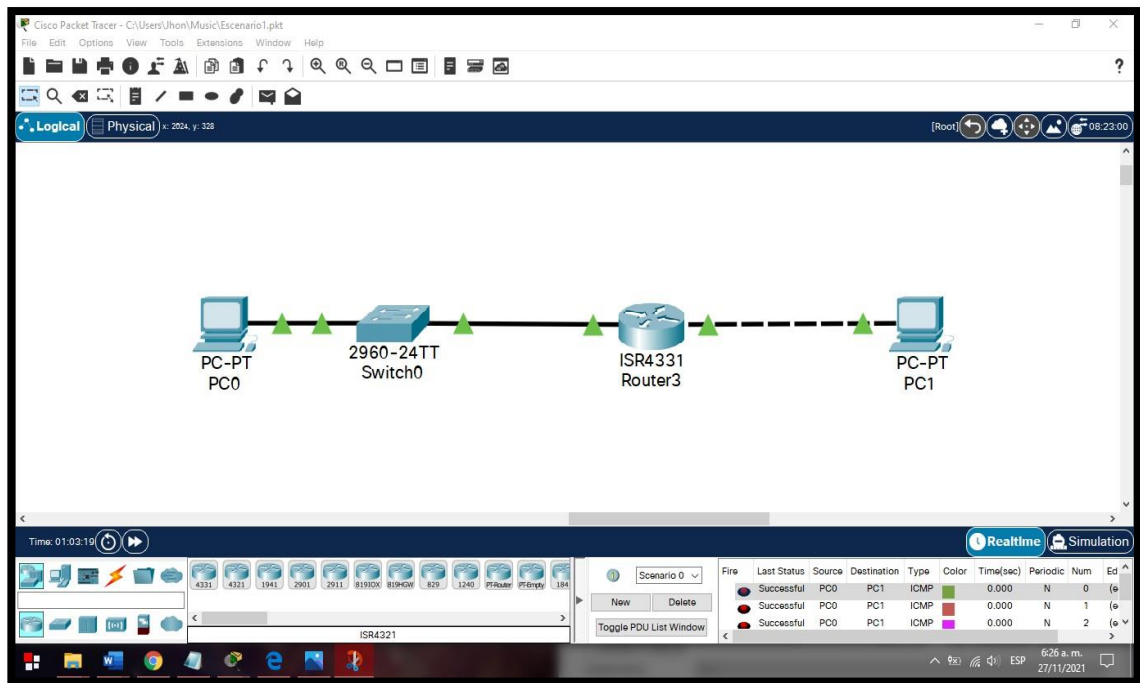
Figura 8 Configuraciones de direcciones para el equipo B.



Fuente. Propia.

Al finalizar la configuración de los elementos mediante un PDU o mensaje se puede comprobar que ambos equipos tengan conexión, de esta forma se puede asegurar que la configuración y asignación de direcciones para cada uno de los dispositivos fue correcta, con esto, el esquema final y la comunicación exitosa se observa a continuación en la figura 9.

Figura 9 Simulación final del primer escenario con conexión entre los equipos A y B.

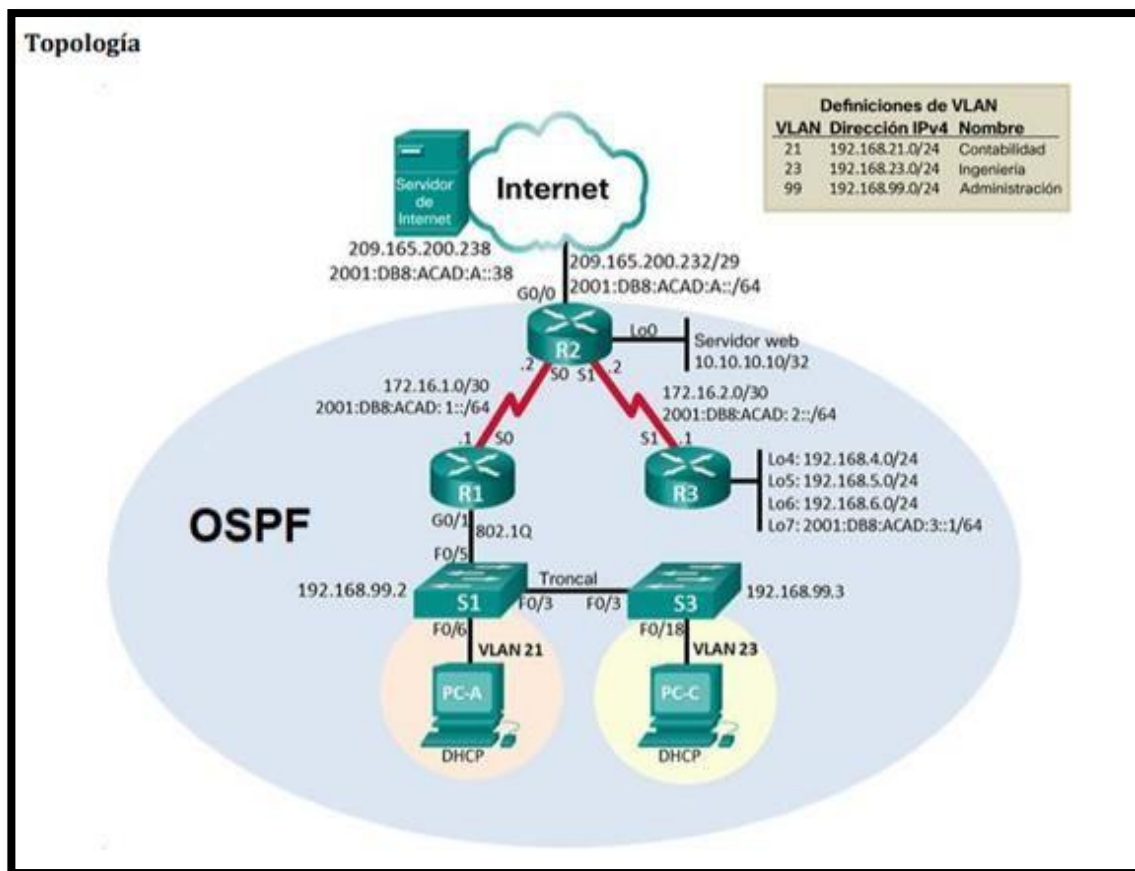


Fuente. *Propia.*

2. Desarrollo del segundo escenario

Para el segundo escenario se nos presenta como ya se mencionó, una topología de tipo WAN, a partir de esta topología se pueden abordar temáticas como seguridad entre switches, routing entre VLAN, protocolo OSPF, DHCP, NTP entre otros, dicha topología se observa a continuación en la figura 10.

Figura 10 Topología de red del segundo escenario.



Fuente. (CISCO, 2017)

Esta red pequeña se configura con el fin de admitir conectividad Ipv4 e Ipv6, seguridad entre los switches, routing entre VLAN, protocolo OSPF, host dinámicos o DHCP entre otros como ya se mencionó.

2.1. Inicialización de dispositivos.

2.1.1. Paso 1: Inicializar y volver a cargar los routers y switches.

Para empezar con la configuración de la red, primero se requiere que los dispositivos se reinicien, entonces se emplean los siguientes comandos:

Tabla 4 Instrucciones y comandos respectivos para el reinicio de los dispositivos del segundo escenario.

Tarea	Comando de IOS
Eliminar el archivo startup-config de todos los routers	Router#enable Router#erase startup - config Continue? [confirm] [Enter] [OK] Erase of nvram: complete Router#
Volver a cargar todos los routers	Router#reload Proceed with reload? [confirm] [Enter] Router
Eliminar el archivo startup-config de todos los switches y eliminar la base de datos de VLAN anterior	Switch#erase startup- config Switch#delete vlan.dat Erasing the nvram filesystem will remove all configuration files! Continue? [confirm] [Enter] [OK] Erase of nvram: complete Switch#

Volver a cargar ambos switches	Switch#reload Proceed with reload? [confirm] [Enter] Switch>
Verificar que la base de datos de VLAN no este en la memoria flash en ambos switches	Switch#show flash: Switch#show vlan brief

Fuente. *Propia.*

Al ejecutarlos en cada uno de los elementos de la simulación nos aseguramos que no tengan configuraciones guardadas.

2.2. Configuración de ajustes básicos en dispositivos.

2.2.1. Paso 1: Configuración de la PC Internet.

A partir de la figura 10, se observa las direcciones IP que están especificadas para la PC Internet por lo tanto se tabula y se calcula su respectiva Gateway y mascara de red.

Tabla 5 Instrucciones y comandos respectivos para el reinicio de los dispositivos del segundo escenario.

Elemento o tarea de configuración	Especificación
Dirección Ipv4	209.165.200.238
Mascara de subred para ipv4	255.255.255.248
Gateway predeterminado	209.165.200.233
Dirección ipv6/subred	2001:DB8:ACAD:A::38/64
Gateway predeterminado ipv6	2001:DB8:ACAD:A::1

Fuente. *Propia.*

2.2.2. Paso 2: Configuración de R1.

Para la configuración del router R1 se lleva a cabo las siguientes tareas.

Tabla 6 Listado de instrucciones o tareas para la configuración del router R1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain - lookup
Nombre del router	Router(config)#hostname R1
Contraseña de exec privilegiada	R1(config)#enable s R1(config)#enable secret class
Contraseña de acceso a la consola	R1(config)#line console 0 R1(config-line)#pas R1(config-line)#password cisco R1(config-line)#login
Contraseña de acceso Telnet	R1(config)#line vty 0 4 R1(config-line)#pass R1(config-line)#password cisco R1(config-line)#login R1(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R1(config)#service password-encryption
Mensaje MOTD	R1(config)#banner motd #se prohíbe El acceso no autorizado red JF#
Interfaz S0/0/0	R1(config)#int s0/1/0 R1(config-if)#description interface hacia el router R2 R1(config-if)#exit R1(config)#ipv6 uni R1(config)#ipv6 unicast - routing R1(config)#int s0/1/0 R1(config-if)#ip address 172.16.1.1 255.255.255.252 R1(config-if)#ipv6 address 2001:DB8:ACAD:1::1/64 R1(config-if)#clock rate 128000 R1(config-if)#no sh R1(config-if)#no shutdown
Rutas predeterminadas	R1(config)#ip route 0.0.0.0.0.0.0s0/1/0 %Default route without gateway, if not a point-to-point interface, may impact performance

R1(config)#ipv6 route ::/0 S0/1/0 R1(config)

Fuente. Propia.

Las configuraciones realizadas en R1 mediante CLI se pueden observar a continuación en la figura

Figura 11 Instrucciones en CLI para la configuración del router R1.

```
Router>enable
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no ip domain-lookup
Router(config)#hostname R1
R1(config)#enable secret class
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#line vty 0 15
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#service password-encryption
R1(config)#banner motd %Se prohíbe el acceso no autorizado%
R1(config)#int s0/0/0
R1(config-if)#description Connection to R2
R1(config-if)#ip address 172.16.1.1 255.255.255.252
R1(config-if)#ipv6 address 2001:db8:acad:1::1/64
R1(config-if)#clock rate 128000
This command applies only to DCE interfaces
R1(config-if)#clock rate 128000
R1(config-if)#no shutdown

%LINK-S-CHANGED: Interface Serial0/0/0, changed state to down
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
^
% Invalid input detected at '^' marker.

R1(config)#ip route 0.0.0.0 0.0.0.0 s0/0/0
%Default route without gateway, if not a point-to-point interface, may impact performance
R1(config)#ipv6 route ::/0 s0/0/0
R1(config)#
```

Fuente. Propia.

2.2.3. Paso 3: Configuración de R2.

Para la configuración del router R2 se lleva a cabo las siguientes tareas.

Tabla 7 Listado de instrucciones o tareas para la configuración del router R2.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ipdomain-lookup
Nombre del router	Router(config)#hostname R2
Contraseña de exec privilegiada	R2(config)#enable s R2(config)#enable secret class
Contraseña de acceso a la consola	R2(config)#line console 0 R2(config-line)#password cisco R2(config-line)#login
Contraseña de acceso Telnet	R2(config)#line vty 0 4 R2(config-line)#pass R2(config-line)#password cisco R2(config-line)#login R2(config-line)#exit
Cifrar las contraseñas de texto no cifrado	R2(config)#service password-encryption
Habilitar el servidor HTTP	R2(config)#ip http server % Invalid input detected at '^'marker
Mensaje MOTD	R2(config)#banner motd #se prohíbe El acceso no autorizado red JF#
Interfaz S0/0/0	R2(config-if)#description interface desde R1 A R2 R2(config-if)#exit R2(config)#ipv6 unicast - routing R2(config)#int s0/1/0 R2(config-if)#ip address 172.16.1.2 255.255.255.252 R2(config-if)#ipv6 address 2001:DB8:ACAD:1::2/64
Interfaz S0/0/1	R2(config)#int S0/1/1 R2(config-if)#description conexión de

	R2 a R3 R2(config-if)#ip address 172.16.2.1 255.255.255.252 R2(config-if)#ipv6 add 2001:DB8:ACAD:2::2/64 R2(config-if)#clock rate 128000 R2(config-if)#no sh
Interfaz G0/0 (simulación de internet)	R2(config)#int g0/0/0 R2(config-if)#description interface hacia internet R2(config-if)#exit R2(config)#in R2(config)#ipv6u R2(config)#ipv6unicast-routing R2(config)#int g0/0/0 R2(config-if)#ip address 209.165.200.233 255.255.255.248 R2(config-if)#ipv6 address 2001:DB8:ACAD:a::1/64 R2(config-if)#nosh
Interfaz loopback 0(servidor web)	Establecer la descripción Establecer dirección IPv4
Rutas predeterminadas	R2(config)#ip route 0.0.0.0 0.0.0.0 g0/0/0 %Default route without gateway, If not a point –to - point interface, may impact performance R2(config)#ipv6 route::/0 g0/0/0

Fuente. *Propia.*

Las configuraciones realizadas en R2 emplean los mismos comandos que las que se utilizaron en R1 salvo por algunas diferencias en la configuración de las interfaces seriales para la simulación de internet y el servidor web que extiende en gran medida las líneas de código y no es estético reportarlas en el documento, por lo cual se omite la ilustración del CLI, la configuración de R2 sin embargo, se puede

revisar ejecutando la simulación “Escenario2.pkt” que se encuentra anexada a este documento.

2.2.4. Paso 4: Configuración de R3.

Para la configuración del router R3 se lleva a cabo las siguientes tareas.

Tabla 8 Listado de instrucciones o tareas para la configuración del router R3.

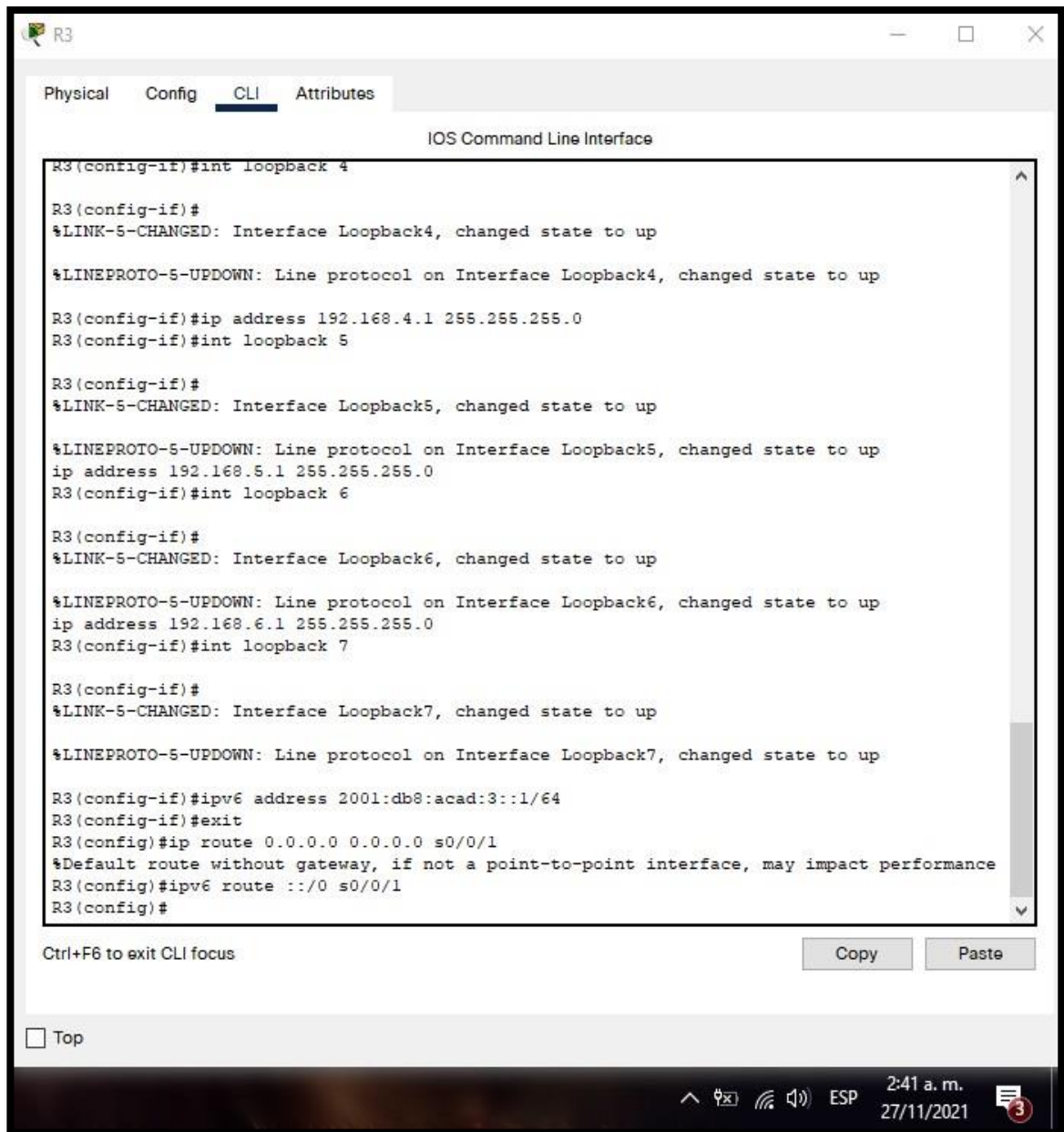
Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Router(config)#no ip domain - lookup
Nombre del router	Router(config)#hostname R3
Contraseña de exec privilegiada	R3(config)#enable secret class
Contraseña de acceso a la consola	R3(config)#line console 0 R3(config-line)#password cisco R3(config-line)#login
Contraseña de acceso Telnet	R3(config)#line vty 0 4 R3(config-line)#pass R3(config-line)#password cisco R3(config-line)#login R3(config-line)#exit
Cifrar Las contraseñas de texto no cifrado	R3(config)#service Password - encryption
Mensaje MOTD	R3(config)#banner motd #se prohíbe El acceso no autorizado red JF#
Interfaz S0/0/1	R3(config-if)#description interface desde R3 a R2 R3(config-if)#exit R3(config)#ipv6 unicast-routing R3(config)#int s0/1/1 R3(config-if)#ip address 172.16.2.2 255.255.255.252 R3(config-if)#ipv6 address 2001:DB8:ACAD:2::1/64 R3(config-if)#no sh

Interfaz loopback 4	R3(config)#int loopback 4 R3(config-if)#31 %LINK-5-CHANGED: Interface Loopback4, changed state To up %LINEPROTO -5-UPDOWN: Line protocol on Interface Loopback4, Changed state to up R3(config-if)#ip add192.168.4.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 5	R3(config)#int loopback 5 R3(config-if)# %LINK – 5 - CHANGED: Interface Loopback5, changed state To up %LINEPROTO -5- UPDOWN: Line protocol on Interface Loopback5, Changed state to up R3(config -if)#ip add 192.168.5.1 255.255.255.0 R3(config-if)#ex
Interfaz loopback 6	R3(config)#int loopback 6 R3(config-if)# %LINK – 5 - CHANGED: Interface Loopback6, changed state To up %LINEPROTO – 5 -UPDOWN: Line protocol on Interface Loopback6, Changed state to up R3(config-if)#ip add 192.168.6.1 255.255.255.0 R3(config-if)#exit
Interfaz loopback 7	R3(config)#int loopback 7 R3(config-if)# %LINK -5-CHANGED: Interface Loopback7, changed state To up %LINEPROTO -5-UPDOWN: Line protocol on Interface Loopback7, Changed state to up R3(config-if)#ipv6 address 2001:DB8:ACAD:3::1/64 R3(config-if)#exit
Rutas predeterminadas	--Procedimiento anterior--

Fuente. *Propia.*

Las ultimas configuraciones realizadas en R3 (debido a que la línea de comandos es muy extensa), se pueden observar a continuación en la figura 12.

Figura 12 Instrucciones en CLI para la configuración del router R3.



```
R3
Physical Config CLI Attributes
IOS Command Line Interface

R3(config-if)#int loopback 4
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback4, changed state to up
R3(config-if)#ip address 192.168.4.1 255.255.255.0
R3(config-if)#int loopback 5
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback5, changed state to up
ip address 192.168.5.1 255.255.255.0
R3(config-if)#int loopback 6
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback6, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback6, changed state to up
ip address 192.168.6.1 255.255.255.0
R3(config-if)#int loopback 7
R3(config-if)#
%LINK-5-CHANGED: Interface Loopback7, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback7, changed state to up
R3(config-if)#ipv6 address 2001:db8:acad:3::1/64
R3(config-if)#exit
R3(config)#ip route 0.0.0.0 0.0.0.0 s0/0/1
%Default route without gateway, if not a point-to-point interface, may impact performance
R3(config)#ipv6 route ::/0 s0/0/1
R3(config)#

Ctrl+F6 to exit CLI focus
Copy Paste
Top
2:41 a. m. 27/11/2021
```

Fuente. Propia.

2.2.5. Paso 5: Configuración de S1.

Para la configuración del switch S1 se lleva a cabo las siguientes tareas.

Tabla 9 Listado de instrucciones o tareas para la configuración del switch S1.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain - lookup
Nombre del switch	Switch(config)#hostnameS1
Contraseña de exec privilegiada	S1(config)#enable s S1(config)#enable secret class
Contraseña de acceso a la consola	S1(config)#line console 0 S1(config-line)#pas S1(config-line)#password cisco S1(config-line)#login
Contraseña de acceso Telnet	S1(config)#line vty 0 15 S1(config-line)#pass S1(config-line)#password cisco S1(config-line)#login S1(config-line)#exi
Mensaje MOTD	S1(config)#banner motd #se prohíbe El acceso no autorizado#

Fuente. *Propia.*

Las configuraciones realizadas en S1 mediante CLI se pueden observar a continuación en la figura 13.

Figura 13 Instrucciones en CLI para la configuración del switch S1.

```

Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#service password-encryption
S1(config)#banner motd %Se prohíbe el acceso no autorizado%
S1(config)#
  
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

2:49 a. m. 27/11/2021

Fuente. *Propia.*

2.2.6. Paso 6: Configuración de S3.

Para la configuración del switch S3 se lleva a cabo las siguientes tareas.

Tabla 10 Listado de instrucciones o tareas para la configuración del switch S3.

Elemento o tarea de configuración	Especificación
Desactivar la búsqueda DNS	Switch(config)#no ip domain-lookup
Nombre del switch	Switch(config)#hostname S3
Contraseña de exec privilegiada	S3(config)#enable secret class
Contraseña de acceso a la consola	S3(config)#line console 0 S3(config-line)#password cisco
Contraseña de acceso Telnet	S3(config)#line vty 0 15 S3(config-line)#password cisco S3(config-line)#login
Mensaje MOTD	S3(config)#banner motd #se prohíbe El acceso no autorizado#

Fuente. *Propia.*

Las configuraciones realizadas en S1 mediante CLI se pueden observar a continuación en la figura 14.

Figura 14 Instrucciones en CLI para la configuración del switch S3.

```
Switch>enable
Switch#conf t
Enter configuration commands, one per line. End with CNIL/Z.
Switch(config)#no ip domain-lookup
Switch(config)#hostname S3
S3(config)#enable secret class
S3(config)#line console 0
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#line vty 0 15
S3(config-line)#password cisco
S3(config-line)#login
S3(config-line)#service password encryption
^
% Invalid input detected at '^' marker.
S3(config-line)#service password-encryption
S3(config)#banner motd %Se prohíbe el acceso no autorizado%
S3(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

2:52 a. m. 27/11/2021

Fuente. Propia.

2.2.7. Paso 7: Verificación de conectividad a la red.

Con la finalidad de comprobar que exista conectividad entre los dispositivos de red, mediante el comando ping se hace test, al realizar dicho procedimiento en la consola de comandos de cada equipo se obtuvo los siguientes resultados.

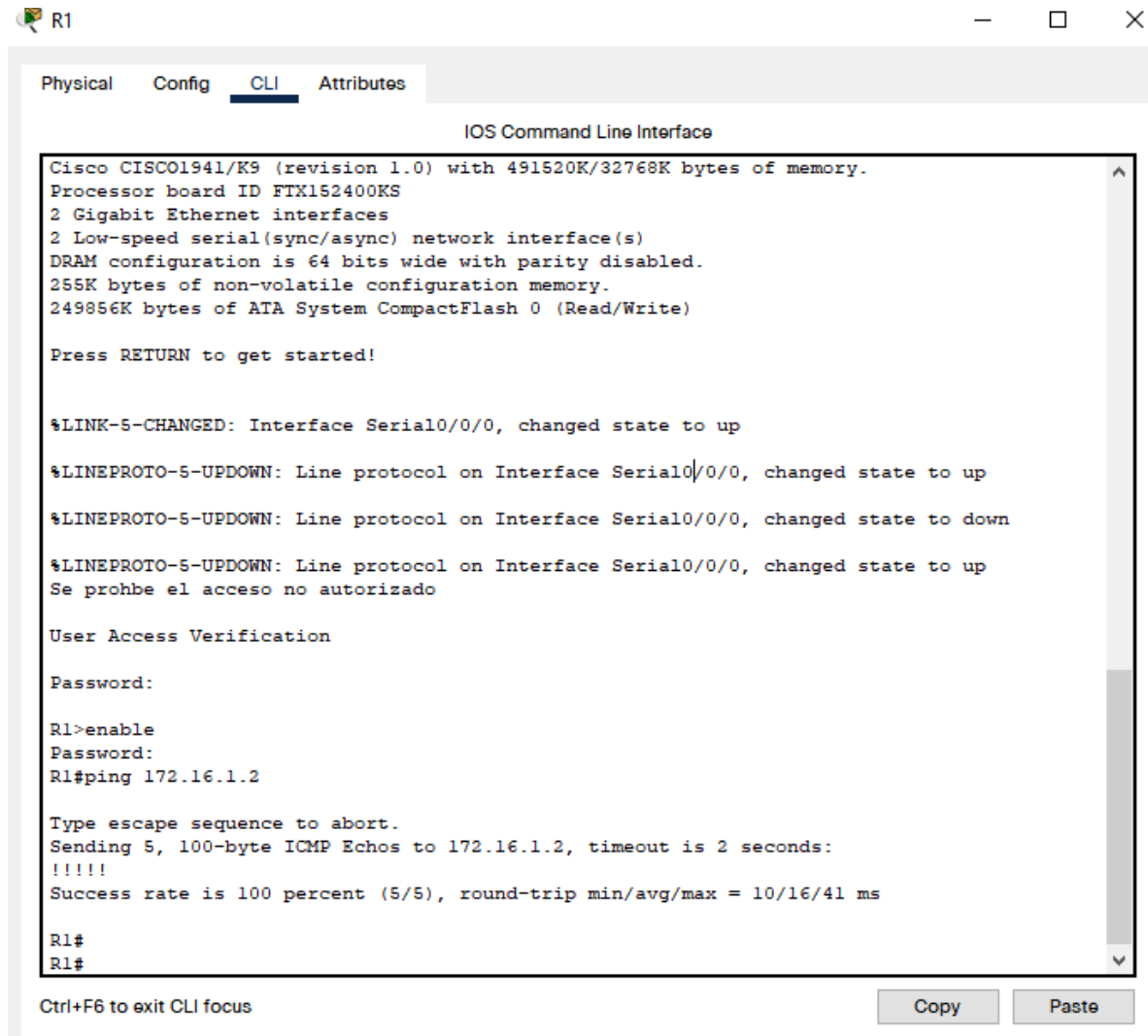
Tabla 11 Resultados de conexión haciendo ping entre los dispositivos configurados.

Desde	A	Dirección IP	Resultados de Ping
R1	R2, S0/0/0	172.16.1.2	Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round - trip

			min/avg/max= 8/12/16 ms
R2	R3, S0/0/1	172.16.2.1	Type escape Sequence to abort. Sending 5, 100-byte ICMP Echos to 172.16.2.2, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round-trip min/avg/max=8/11/16 ms
PC de Internet	Gateway predeterminada	209.165.200.233	Ping statistics For 209.165.200.233: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate Round trip times in milli- seconds: minimum = 0ms, Maximum = 95ms, Average = 23ms IPV6 Ping statistics for 2001:DB8:ACAD:A::1: Packets: Sent = 4 Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli- seconds: Minimum = 0ms, Maximum = 64ms, Average = 16ms

Fuente. *Propia.*

Figura 15 Verificación de la conexión de la red entre R1 a R2.



```
Cisco CISCO1941/K9 (revision 1.0) with 491520K/32768K bytes of memory.
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
2 Low-speed serial(sync/async) network interface(s)
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Se prohbe el acceso no autorizado

User Access Verification

Password:

R1>enable
Password:
R1#ping 172.16.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/16/41 ms

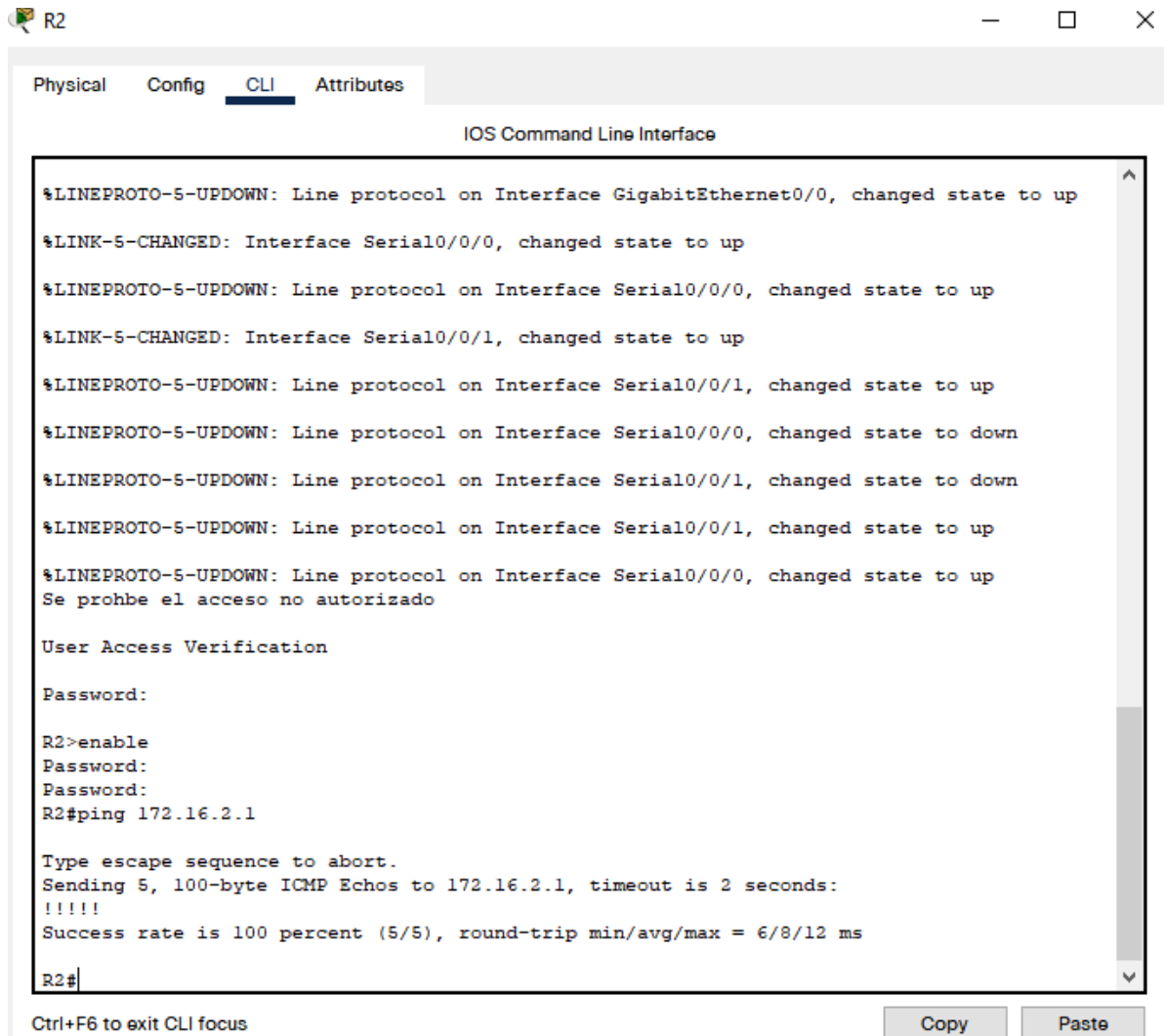
R1#
R1#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Fuente. *Propia.*

Figura 16 Verificación de la conexión de la red entre R2 a R3.



The screenshot shows the CLI window of router R2. The window has tabs for Physical, Config, CLI (selected), and Attributes. The title bar says 'R2'. The main area is titled 'IOS Command Line Interface'. It displays a series of system messages: '%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up', '%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up', '%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up', '%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up', '%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up', '%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down', '%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down', '%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up', and '%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up'. Below these is a 'User Access Verification' section with a 'Password:' prompt. The user enters 'enable' at the 'R2>' prompt, followed by another 'Password:' prompt. Then, the user enters 'ping 172.16.2.1' at the 'R2#' prompt. The output shows 'Type escape sequence to abort.', 'Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:', '!!!!', and 'Success rate is 100 percent (5/5), round-trip min/avg/max = 6/8/12 ms'. The prompt 'R2#' is visible at the bottom. At the bottom of the window, there is a status bar with 'Ctrl+F6 to exit CLI focus' on the left and 'Copy' and 'Paste' buttons on the right.

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
%LINK-5-CHANGED: Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/0, changed state to up
Se prohbe el acceso no autorizado

User Access Verification

Password:

R2>enable
Password:
Password:
R2#ping 172.16.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.2.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/8/12 ms

R2#
```

Fuente. *Propia.*

Figura 17 Verificación de la conexión de la red entre PC internet a Gateway predeterminado.

Fuente. *Propia.*

Nota: Quizá sea necesario deshabilitar el firewall de las computadoras para que los pings se realicen correctamente.

2.3. Configuración de seguridad de switches, VLAN y routing entre VLAN.

2.3.1. Paso 1: Configuración de S1.

Para la configuración del switch S1 se lleva a cabo las siguientes tareas.

Tabla 12 Listado de instrucciones para configuraciones de seguridad en el switch S1.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S1(config)#vlan21 S1(config-vlan)#name contabilidad S1(config-vlan)#vlan 23 S1(config-vlan)#name ingenieria S1(config-vlan)#vlan 99 S1(config-vlan)#name administracion S1(config-vlan)#
Asignar la dirección IP de administración	S1(config)#int vlan 99 S1(config-if)# %LINK-5-CHANGED: Interface Vlan99,changed state to up S1(config-if)#ip address 192.168.99.2 255.255.255.0 S1(config-if)#no sh S1(config-if)#no shutdown S1(config-if)#exit
Asignar el Gateway predeterminado	S1(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S1(config)#int f0/3 S1(config-if)#sw mode trunk S1(config-if)# %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state To down %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up %LINEPROTO-5 -UPDOWN:Line protocol on Interface Vlan99, changed State to up S1(config-if)#sw trunk Native vlan 1 S1(config-if)#exit
Forzar el enlace troncal en la interfaz F0/5	S1(config)#int f0/5 S1(config-if)#sw mode trunk S1(config-if)#switchport trunk native Vlan 1 S1(config-if)#exit
Configurar el resto de puertos como puertos de acceso	S1(config)#int range f0/1-f0/2 S1(config-if-range)#sw mode acc S1(config-if-range)#sw mode access S1(config-if-range)#int range f0/7-f0/24

	S1(config-if-range)#sw mode access S1(config-if-range)#
Asignar F0/6 a la VLAN 21	S1(config)#intf0/6 S1(config-if)#sw access vlan 21
Apagar todos los puertos sin usar	S1(config-if)#inrange f0/7-f0/24 S1(config-if-range)#sh

Fuente. *Propia.*

A continuación, se observa la implementación de dichas instrucciones en CLI.

Figura 18 Instrucciones de seguridad en CLI para la configuración del switch S1.

```

S1#
%SYS-5-CONFIG_I: Configured from console by console

S1#conf term
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)#int vlan 99
S1(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

S1(config-if)#ip address 192.168.99.2 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#exit
S1(config)#ip default-gateway 192.168.99.1
S1(config)#int f0/3
S1(config-if)#switchport mode trunk

S1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 1
S1(config-if)#int range f0/1-2, f0/4, f0/6-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#int f0/6
S1(config-if)#switchport access vlan 21
S1(config-if)#
S1#
%SYS-5-CONFIG_I: Configured from console by console

S1>show vlan

VLAN Name                Status    Ports
-----
1    default                active    Fa0/1, Fa0/2, Fa0/4, Fa0/7
                                           Fa0/8, Fa0/9, Fa0/10, Fa0/11
                                           Fa0/12, Fa0/13, Fa0/14, Fa0/15
                                           Fa0/16, Fa0/17, Fa0/18, Fa0/19
                                           Fa0/20, Fa0/21, Fa0/22, Fa0/23
                                           Fa0/24, Gig0/1, Gig0/2
21   Contabilidad            active    Fa0/6
23   Ingenieria              active
99   Administracion           active
1002 fddi-default             active
1003 token-ring-default     active
1004 fddinet-default        active
1005 trnet-default          active

VLAN Type  SAID      MTU   Parent RingNo BridgeNo Stp  BrdgMode Transl Trans2
-----
1    enet  100001   1500  -     -     -     -   -       C      0
21   enet  100021   1500  -     -     -     -   -       C      0
23   enet  100023   1500  -     -     -     -   -       C      0
--More--

```

Fuente. *Propia.*

2.3.2. Paso 2: Configuración de S3.

Para la configuración del switch S3 se lleva a cabo las siguientes tareas.

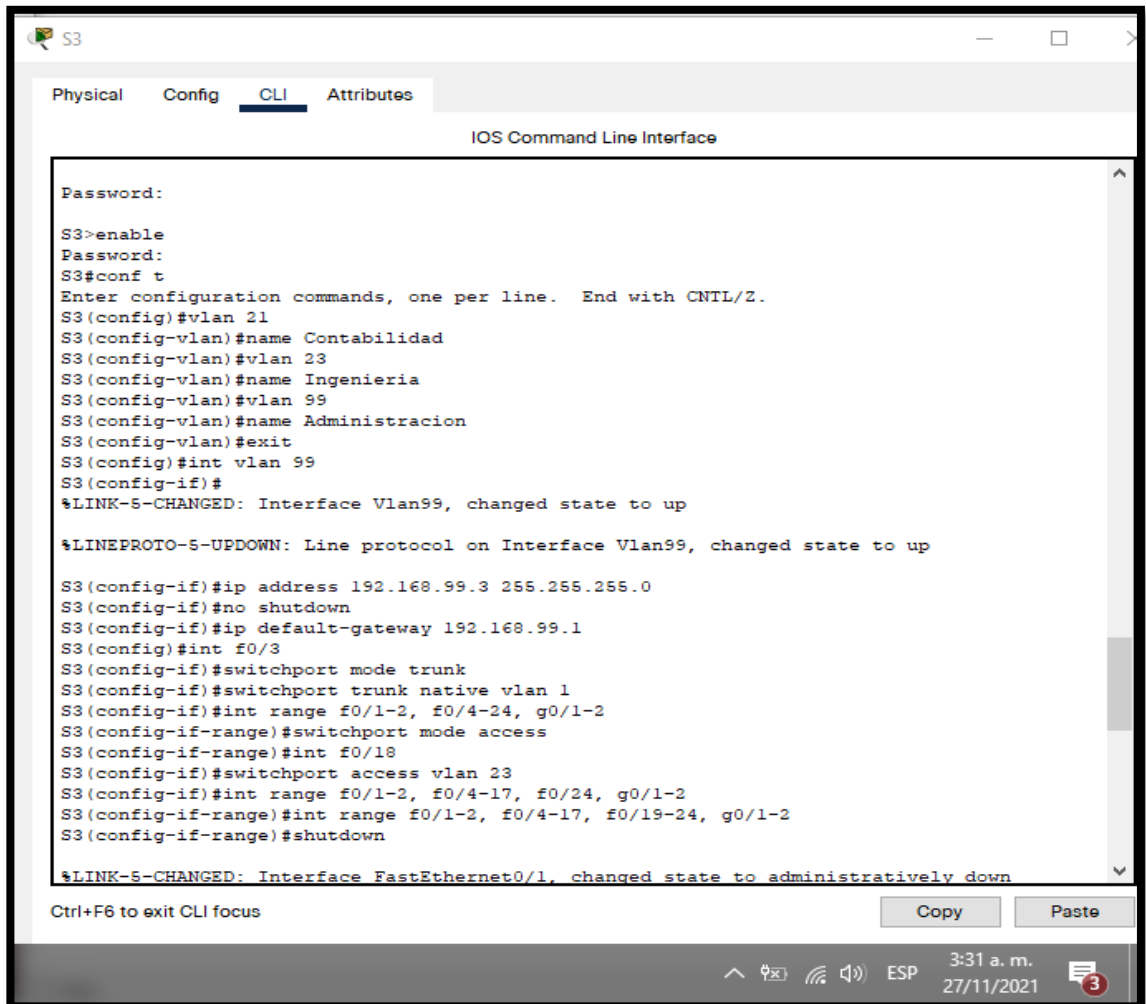
Tabla 13 Listado de instrucciones para configuraciones de seguridad en el switch S3.

Elemento o tarea de configuración	Especificación
Crear la base de datos de VLAN	S3(config)#vlan21 S3(config-vlan)#name contabilidad S3(config-vlan)#vlan 23 S3(config-vlan)#name ingenieria S3(config-vlan)#vlan 99 S3(config-vlan)#name administracion S3(config-vlan)#exit
Asignar la dirección IP de administración	S3(config)#int vlan 99 S3(config-if)#%LINK-5-CHANGED: Interface Vlan99,changed state to Up %LINEPROTO -5-UPDOWN: Line protocol on Interface Vlan99, changed state to up S3(config-if)#ipadd192.168.99.3 255.255.255.0 S3(config-if)#nosh S3(config-if)#exit
Asignar el Gateway predeterminado	S3(config)#ip default-gateway 192.168.99.1
Forzar el enlace troncal en la interfaz F0/3	S3(config)#int f0/3 S3(config-if)#sw mode trunk S3(config-if)#sw trunk native vlan 1 S3(config-if)#exit
Configurar el resto de puertos como puertos de acceso	S3(config)#int range f0/1-f0/2 S3(config-if-range)#sw mode access S3(config-if-range)#int range f0/7-f0/24 S3(config-if-range)#sw mode access S3(config-if-range)#exit
Asignar F0/18 a la VLAN 21	S3(config)#int f0/18 S3(config-if)#sw acc vlan 21
Apagar todos los puertos sin usar	S3(config-if)#int range f0/7 - f0/17 S3(config-if-range)#sh

Fuente. *Propia.*

A continuación, se observa la implementación de dichas instrucciones en CLI.

Figura 19 Instrucciones de seguridad en CLI para la configuración del switch S3.



```

S3
Physical Config CLI Attributes
IOS Command Line Interface

Password:
S3>enable
Password:
S3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#vlan 21
S3(config-vlan)#name Contabilidad
S3(config-vlan)#vlan 23
S3(config-vlan)#name Ingenieria
S3(config-vlan)#vlan 99
S3(config-vlan)#name Administracion
S3(config-vlan)#exit
S3(config)#int vlan 99
S3(config-if)#
%LINK-5-CHANGED: Interface Vlan99, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up

S3(config-if)#ip address 192.168.99.3 255.255.255.0
S3(config-if)#no shutdown
S3(config-if)#ip default-gateway 192.168.99.1
S3(config)#int f0/3
S3(config-if)#switchport mode trunk
S3(config-if)#switchport trunk native vlan 1
S3(config-if)#int range f0/1-2, f0/4-24, g0/1-2
S3(config-if-range)#switchport mode access
S3(config-if-range)#int f0/18
S3(config-if)#switchport access vlan 23
S3(config-if)#int range f0/1-2, f0/4-17, f0/24, g0/1-2
S3(config-if-range)#int range f0/1-2, f0/4-17, f0/19-24, g0/1-2
S3(config-if-range)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down

Ctrl+F6 to exit CLI focus
Copy Paste
3:31 a. m.
27/11/2021
```

Fuente. Propia.

2.3.3. Paso 3: Configuración de R1.

Para la configuración del router R1 se lleva a cabo las siguientes tareas.

Tabla 14 Listado de instrucciones para configuraciones de seguridad en el router R1.

Elemento o tarea de configuración	Especificación
Configurar la subinterfaz 802.1Q .21 en G0/1	R1(config)#int g0/0/1.21 R1(config-subif)#%LINK-5-CHANGED: Interface GigabitEthernet0/0/1.21, Changed state to up %LINEPROTO -5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.21, Changed state to up R1(config-subif)#descri R1(config-subif)#description LAN contabilidad R1(config-subif)#enc dot1q 21 R1(config-subif)#ip add R1(config-subif)#ip address 192.168.21.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .23 en G0/1	R1(config)#int g0/0/1.23 R1(config-subif)# %LINK – 5 - CHANGED: Interface GigabitEthernet0/0/1.23, changed State to up 38 %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1.23,changed state To up R1(config-subif)#description LAN ingenieria R1(config-subif)#enc dot1q 23 R1(config-subif)#ip address 192.168.23.1 255.255.255.0 R1(config-subif)#exit
Configurar la subinterfaz 802.1Q .99 en G0/1	R1(config)#int g0/0/1.99 R1(config-subif)# %LINK-5-CHANGED: Interface GigabitEthernet0/0/1.99, Changed state to up %LINEPROTO-5-UPDOWN: Line protocol on Interface

	GigabitEthernet0/0/1.99,changed state To up R1(config-subif)#description LAN administracion R1(config-subif)#enc dot1q 99 R1(config-subif)#ip address 192.168.99.1 255.255.255.0 R1(config-subif)#exit
Activar la interfaz G0/1	R1(config)#int g0/0/1 R1(config-if)#no sh

Fuente. *Propia.*

A continuación, se observa la implementación de dichas instrucciones en CLI.

Figura 20 Instrucciones de seguridad en CLI para la configuración del router R1.

The screenshot shows the CLI of router R1. The interface has tabs for Physical, Config, CLI (selected), and Attributes. The main window displays the following text:

```

Se prohíbe el acceso no autorizado
User Access Verification
Password:
R1>enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int g0/1.21
R1(config-subif)#description VLAN 21
R1(config-subif)#encapsulation dot1q 21
R1(config-subif)#ip address 192.168.21.1 255.255.255.0
R1(config-subif)#int g0/1.23
R1(config-subif)#description VLAN 23
R1(config-subif)#encapsulation dot1q 23
R1(config-subif)#ip address 192.168.23.1 255.255.255.0
R1(config-subif)#int g0/1.99
R1(config-subif)#description VLAN 99
R1(config-subif)#encapsulation dot1q 99
R1(config-subif)#ip address 192.168.99.1 255.255.255.0
R1(config-subif)#int g0/1
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed state to up
%LINK-5-CHANGED: Interface GigabitEthernet0/1.21, changed state to up

```

At the bottom, there are buttons for Copy and Paste, and a status bar showing the time as 3:39 a.m. on 27/11/2021.

Fuente. *Propia.*

2.3.4. Paso 4: Verificación de la conectividad de la red.

Al igual que en el inciso anterior, se comprueba la conectividad entre los switches y R1 haciendo ping, a continuación, se presentan los resultados.

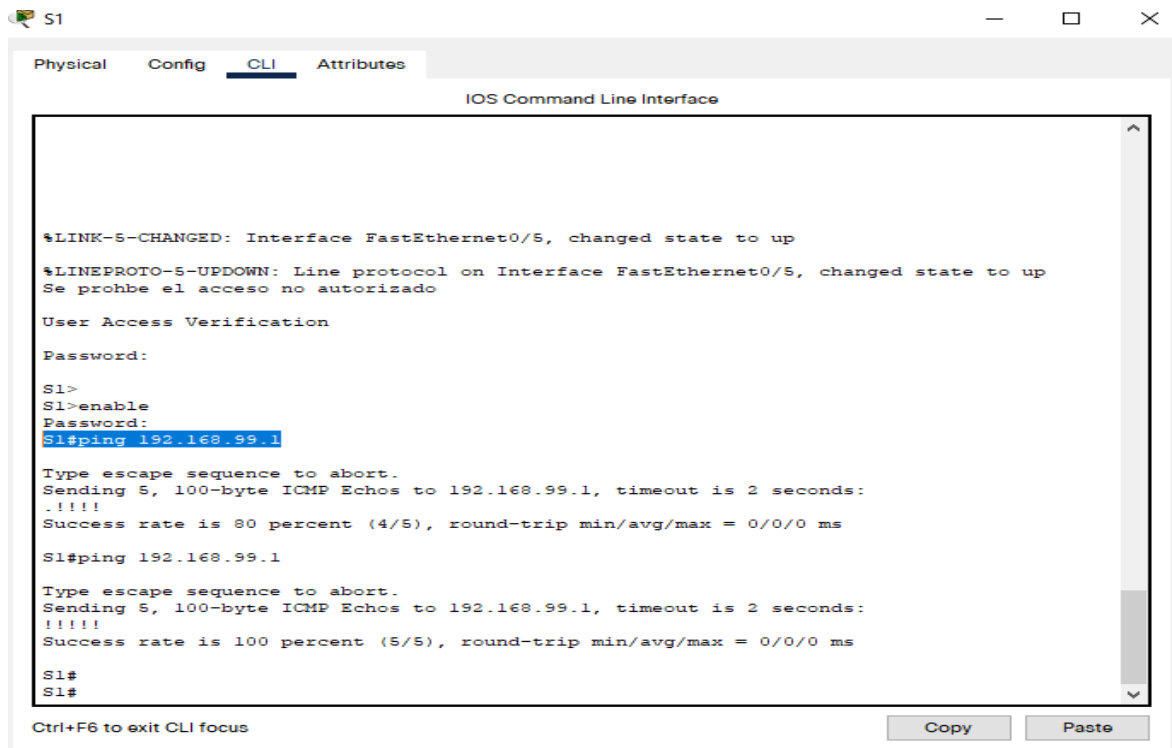
Tabla 15 Resultados de conexión haciendo ping entre los dispositivos configurados para seguridad.

Desde	A	Dirección IP	Resultados de Ping
S1	R1, dirección VLAN 99	192.168.99.1	S1#ping 192.168.99.1 Type escape sequence to abort.Sending 5,100 - Byte ICMP Echos to 192.168.99.1, Timeout is 2 seconds: 39 !!!! Success rate is 100 percent (5/5), round-trip min/avg/max=0/2/6 ms
S3	R1, dirección VLAN 99	192.168.99.1	S3#ping 192.168.99.1 Type escape Sequence to abort.Sending 5,100 -byte ICMP Echos to 92.168.99.1,timeout is 2 seconds: !!!!! Success rate is 100 Percent (5/5), round- trip min/avg/max=0/0/0 ms

S1	R1, dirección VLAN 21	192.168.21.1	Type escape Sequence to abort. Sending 5, 100-byte ICMP Echos to 192.168.21.1,timeout is 2 seconds: !!!!! Success rate is 100 Percent (5/5),round -trip min/avg/max =0/0/0 ms
S3	R1, dirección VLAN 23	192.168.23.1	S3#ping 192.168.23.1 Type Escape sequence To abort Sending 5,100 –byte ICMP Echos to 192.168.23.1,timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round trip min/avg/max = 0/0/0 ms

Fuente. *Propia.*

Figura 21 Verificación de la conectividad de la red desde S1 a R1 VLAN 99



The screenshot shows the CLI of switch S1. The tabs at the top are Physical, Config, CLI (selected), and Attributes. The title bar says 'S1' and 'IOS Command Line Interface'. The terminal output shows the following sequence of events:

```
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
Se prohbe el acceso no autorizado

User Access Verification

Password:
S1>
S1>enable
Password:
S1#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

S1#ping 192.168.99.1

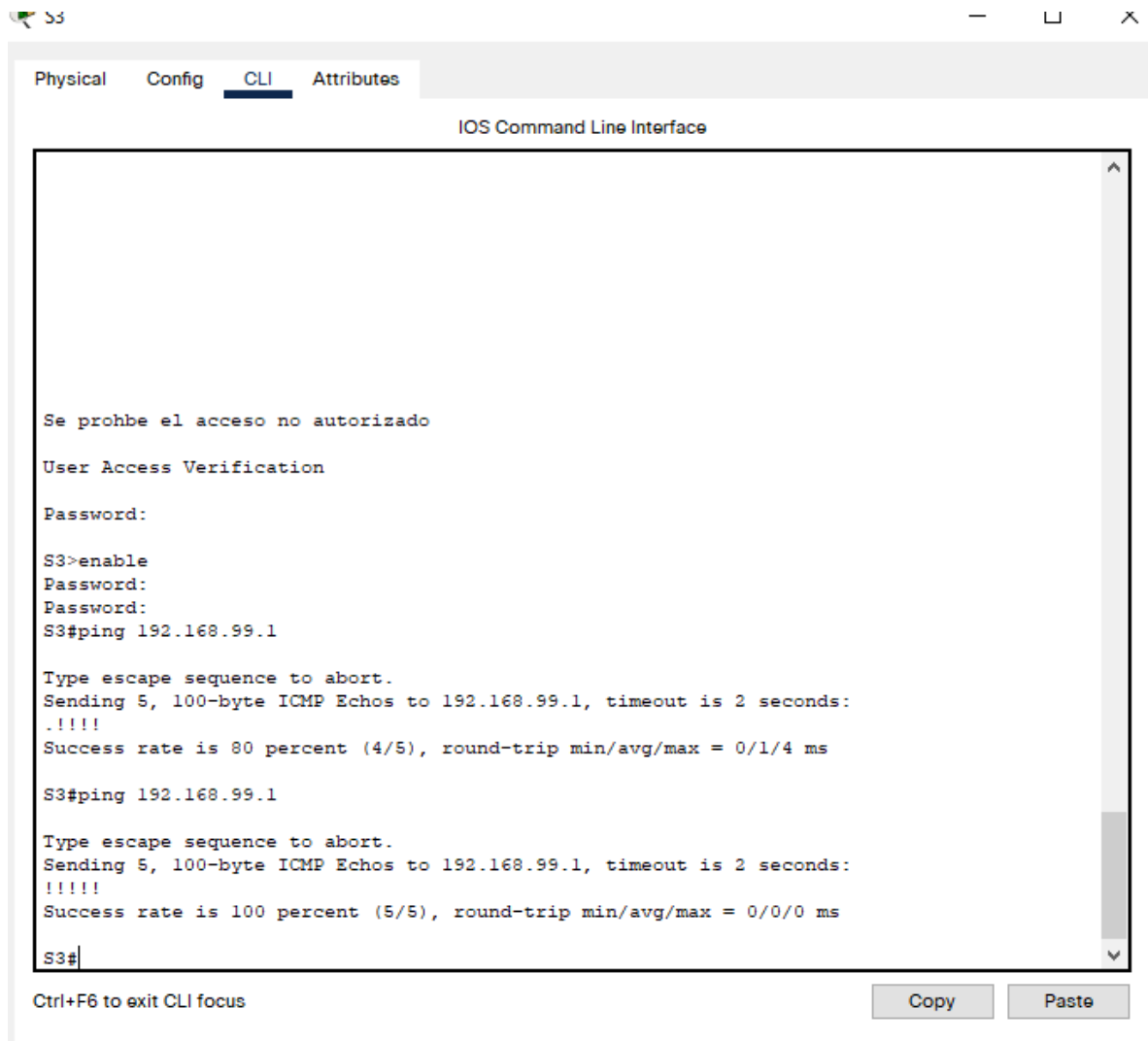
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S1#
S1#
```

At the bottom of the window, there is a status bar that says 'Ctrl+F6 to exit CLI focus' and two buttons labeled 'Copy' and 'Paste'.

Fuente. *Propia.*

Figura 22 Verificación de la conectividad de la red desde S3 a R1 VLAN 99.



```
Physical  Config  CLI  Attributes

IOS Command Line Interface

Se prohbe el acceso no autorizado
User Access Verification
Password:
S3>enable
Password:
Password:
S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/1/4 ms

S3#ping 192.168.99.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.99.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

S3#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Fuente. Propia.

Figura 23 Verificación de la conectividad de la red desde S3 a R1 VLAN 21.

Fuente. *Propia.*

Figura 24 Verificación de la conectividad de la red desde S1 a R1 VLAN 21

Fuente. *Propia.*

A continuación, se observa la implementación de dichas instrucciones en CLI.

Figura 25 Instrucciones en CLI para configuraciones de protocolo OSPF en R1.

```
R1(config-if)#exit
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#do show ip route connected
C    172.16.1.0/30 is directly connected, Serial0/0/0
C    192.168.21.0/24 is directly connected, GigabitEthernet0/1.21
C    192.168.23.0/24 is directly connected, GigabitEthernet0/1.23
C    192.168.99.0/24 is directly connected, GigabitEthernet0/1.99

R1(config-router)#network 172.16.1.0
R1(config-router)#network 192.168.21.0
R1(config-router)#network 192.168.23.0
R1(config-router)#network 192.168.99.0
R1(config-router)#passive-interface g0/1.21
R1(config-router)#passive-interface g0/1.23
R1(config-router)#passive-interface g0/1.99
R1(config-router)#no auto-summary
R1(config-router)#
```

Fuente. *Propia.*

2.4. Configuración de protocolo de routing dinámico OSPF.

2.4.1. Paso 1: Configuración OSPF en R1.

Las tareas de configuración del protocolo OSPF para R1.

Tabla 16 Listado de instrucciones para configuraciones de protocolo OSPF en R1.

Elemento o tarea de configuración	Especificación.
Configurar OSPF área 0	R1(config)#router ospf 36
Anunciar las redes conectadas directamente	R1(config-router)#network 192.168.21.0 0.0.0.255 Área 0 R1(config-router)#network 192.168.23.0 0.0.0.255 Área 0 R1(config-router)#network 192.168.99.0 0.0.0.255 Área 0 R1(config-router)#network 172.16.1.0 0.0.0.3 area 0
Establecer todas las interfaces LAN Como pasivas	R1(config-router)#passive-interface g0/0/1 R1(config-router)#passive-interface g0/0/1.21 R1(config-router)#passive-interface g0/0/1.23 R1(config-router)#passive-interface g0/0/1.99
Desactive la sumarizacion automática.	No se puede descativar sumarizacion automática

Fuente. *Propia.*

2.4.2. Paso 2: Configuración OSPF en R2.

Las tareas de configuración del protocolo OSPF para R2.

Tabla 17 Listado de instrucciones para configuraciones de protocolo OSPF en R1.

Elemento o tarea de configuración	Especificación.
Configurar OSPF área 0	R2(config)#router ospf 36
Anunciar las redes conectadas directamente	R2(config-router)#network 10.10.10.10 0.0.0.0 area 0 R2(config-router)#network 172.16.1.0 0.0.0.3 area 0 42 R2(config-router)# 01:34:05: %OSPF-5 -ADJCHG:Process 36, Nbr 192.168.99.1 on Serial0/1/0 from LOADING to FULL, Loading Done R2(config-router)#network 172.16.2.0 0.0.0.3 area 0
Establecer la interfaz LAN como pasiva	R2(config-router)#passive-interface Loopback 0
Desactive la sumarizacion automática.	No se puede desactivar sumarizacion Automática en ospf

Fuente. *Propia.*

A continuación, se observa la implementación de dichas instrucciones en CLI.

Figura 26 Instrucciones en CLI para configuraciones de protocolo OSPF en R2.

```

R2>enable
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf
R2(config-router)#version 2
R2(config-router)#do show ip route connected
C 10.10.10.10/32 is directly connected, Loopback0
C 172.16.1.0/30 is directly connected, Serial0/0/0
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 209.165.200.232/29 is directly connected, GigabitEthernet0/0

R2(config-router)#network 10.10.10.10
R2(config-router)#network 172.16.1.0
R2(config-router)#network 172.16.2.0
R2(config-router)#passive-interface loopback 0
R2(config-router)#no auto-summary
R2(config-router)#
  
```

Fuente. *Propia.*

2.4.3. Paso 3: Configuración OSPFv3 en R3.

Las tareas de configuración del protocolo OSPFv3 para R3.

Tabla 18 Listado de instrucciones para configuraciones de protocolo OSPFv3 en R3.

Elemento o tarea de configuración	Especificación.
Configurar OSPF área 0	R3(config)#ipv6 router ospf 37
Anunciar las redes conectadas directamente	R3(config - rtr)#router-id 2.2.2.2 R3(config-rtr)#exit R3(config)#int s0/1/1 R3(config-if)#ipv6 ospf 37 area 0 R3(config-if)#exit R3(config)#
Establecer la interfaz LAN como pasiva	R3(config)#int loopback 7 R3(config-if)#ipv6 ospf 37 area 0 R3(config-if)#exit R3(config)#ipv6 router ospf 37 R3(config-rtr)#passive R3(config-rtr)#passive-interface lo 4 R3(config-rtr)#passive-interface lo 5 R3(config-rtr)#passive-interface lo 6 R3(config-rtr)#
Desactive la sumarización automática.	No se puede

Fuente. *Propia.*

A continuación, se observa la implementación de dichas instrucciones en CLI.

Figura 27 Instrucciones en CLI para configuraciones de protocolo OSPFv3 en R3.

```

R3>enable
Password:
R3#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#do show ip route connected
C 172.16.2.0/30 is directly connected, Serial0/0/1
C 192.168.4.0/24 is directly connected, Loopback4
C 192.168.5.0/24 is directly connected, Loopback5
C 192.168.6.0/24 is directly connected, Loopback6

R3(config-router)#network 172.16.2.0
R3(config-router)#network 192.168.4.0
R3(config-router)#network 192.168.5.0
R3(config-router)#network 192.168.6.0
R3(config-router)#passive-interface loopback 4
R3(config-router)#passive-interface loopback 5
R3(config-router)#passive-interface loopback 6
R3(config-router)#no auto-summary
R3(config-router)#

```

Ctrl+F6 to exit CLI focus

Copy Paste

3:59 a. m. 27/11/2021

Fuente. Propia.

2.4.4. Paso 4: Verificación de la información de OSPF.

En este inciso se establece que comandos de CLI nos permiten conocer que el protocolo este en funcionamiento, por lo que se completa dicha tabla y se comprueba en el CLI obteniendo un resultado satisfactorio.

Tabla 19 Listado de comandos para verificar el funcionamiento del protocolo OSPF.

Pregunta	Respuesta
Con que comando se muestra la ID del proceso OSPF, la ID del router, ¿las redes de routing y las interfaces pasivas configuradas en un router?	Con el comando “ <i>show ip protocols</i> ”

¿Qué comando muestra solo las rutas OSPF?	Con el comando “ <i>show ip route rip</i> ”
¿Qué comando muestra la sección de OSPF de la configuración en ejecución?	Con el comando “ <i>show run</i> ”

Fuente. *Propia*.

2.5. Implementación de DHCP y NAT para IPv4.

2.5.1. Paso 1: Configuración de R1 como servidor de DHCP para VLAN 21 Y 23.

Las tareas de configuración para servidor DHCP y VLAN 21/23 son:

Tabla 20 Listado de instrucciones para la configuración de DHCP en R1.

Elemento o tarea de configuración	Especificación
Reservar las primeras 20 direcciones IP en la VLAN 21 para configuraciones estáticas.	R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
Reservar las primeras 20 direcciones IP en la VLAN 23 para configuraciones estáticas.	R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
Crear un pool de DHCP para la VLAN 21	R1(config)#ip dhcp pool ACCT R1(dhcp-config)#network 192.168.21.0 255.255.255.0 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#dns-

	R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#defa R1(dhcp-config)#default-router 192.168.21.1 R1(dhcp-config)#exit R1(config)#ip dhcp pool ENGR R1(dhcp-config)#network 192.168.23.0 255 .255.255.0 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna-sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#
Crear un pool de DHCP para la VLAN 23	R1(config)#ip dhcp pool ENGR R1(dhcp-config)#network 192.168.23.0 255.255.255.0 R1(dhcp-config)#dns-server 10.10.10.10 R1(dhcp-config)#domain-name ccna- sa.com R1(dhcp-config)#default-router 192.168.23.1 R1(dhcp-config)#

Fuente. *Propia*.

A continuación, se observa la implementación de dichas instrucciones en CLI.

Figura 28 Instrucciones en CLI para la configuración de DHCP en R1.

```

R1>enable
Password:
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ip dhcp excluded-address 192.168.21.1 192.168.21.20
R1(config)#ip dhcp excluded-address 192.168.23.1 192.168.23.20
R1(config)#ip dhcp pool ACCT
R1(dhcp-config)#network 192.168.21.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.21.1
R1(dhcp-config)#dns-server 10.10.10.10
R1(dhcp-config)#ip dhcp pool ENGNR
R1(dhcp-config)#network 192.168.23.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.23.1
R1(dhcp-config)#

```

Ctrl+F6 to exit CLI focus

Copy Paste

4:18 a. m.
27/11/2021

Fuente. *Propia.*

2.5.2. Paso 2: Configuración de NAT estática y dinámica en R2.

Las tareas de configuración para la NAT estática y dinámica en R2 son:

Tabla 21 Listado de instrucciones para la configuración de NAT estática y dinámica en R2.

Elemento o tarea de configuración	Especificación
Crear una base de datos local con una cuenta de usuario	Usuario: webuser Contraseña:12345 Privilegio: 15
Crear una NAT estática al servidor web	Dirección global interna: 209.165.200.233
Configurar la NAT dinámica dentro de una ALC privada	--
Defina el pool de direcciones IP publicas utilizables	Nombre: INTERNET
Definir la traducción de NAT dinámica	

Fuente. *Propia.*

A continuación, se observa la implementación de dichas instrucciones en CLI.

Figura 29 Instrucciones en CLI para la configuración de NAT estática y dinámica en R2.

```
R2>enable
Password:
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#username webuser privilege 15 secret cisco12345
R2(config)#ip nat inside source static 10.10.10.10 209.165.200.237
R2(config)#int g0/0
R2(config-if)#ip nat outside
R2(config-if)#int s0/0/0
R2(config-if)#ip nat inside
R2(config-if)#int s0/0/1
R2(config-if)#ip nat inside
R2(config-if)#exit
R2(config)#access-list 1 permit 192.168.21.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.23.0 0.0.0.255
R2(config)#access-list 1 permit 192.168.4.0 0.0.3.255
R2(config)#ip nat pool INTERNET 209.165.200.233 209.165.200.236 netmask 255.255.255.248
R2(config)#ip nat inside list 1 pool INTERNET
^
% Invalid input detected at '^' marker.

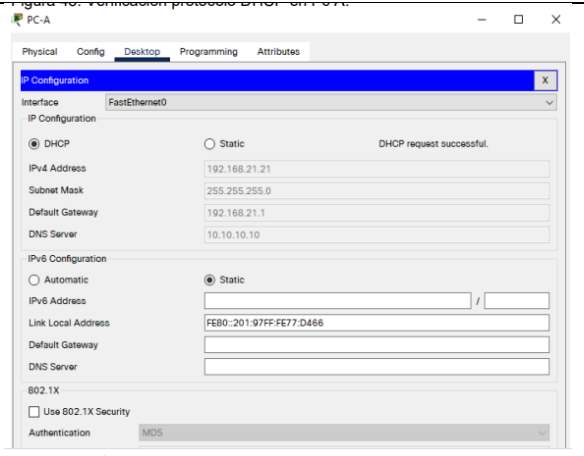
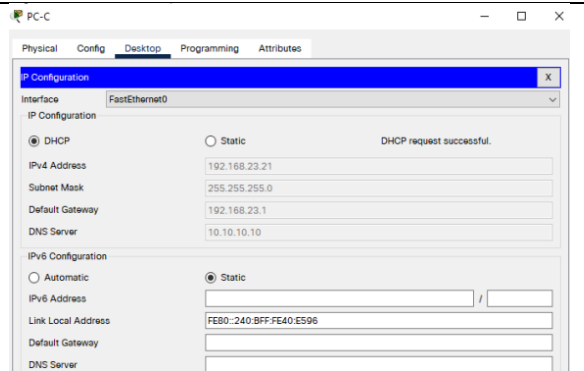
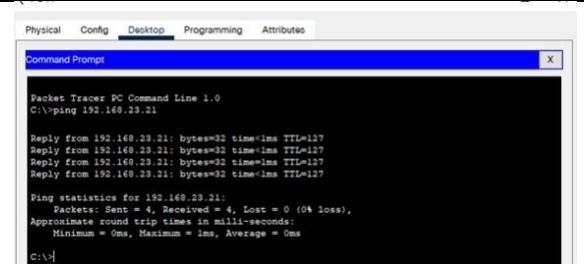
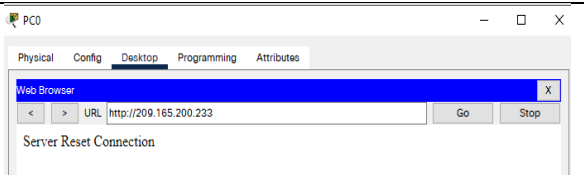
R2(config)#ip nat inside source list 1 pool INTERNET
R2(config)#
```

Fuente. *Propia.*

2.5.3. Paso 3: Verificación de protocolo DHCP y NAT estática.

En este inciso se establece que comandos de CLI nos permiten verificar el protocolo DHCP así como la NAT estática completando dicha tabla, además de comprobar en CLI obteniendo un resultado correcto.

Tabla 22 Listado de comandos para la verificación del protocolo DHCP y NAT estática y dinámica en R2.

Prueba	Resultados
Verificar que la PC-A haya adquirido información de IP del servidor DHCP	
Verificar que la PC-C haya adquirido información de IP del servidor DHCP	
Verificar que la PC-a pueda hacer ping a la PC-C	
Utilizar un navegador web en la computadora de Internet para acceder al servidor web (209.165.200.233).	

Fuente. *Propia.*

2.6. Configuración de NTP.

Para la configuración de NTP se tienen las siguientes tareas:

Tabla 23 Listado de instrucciones para la configuración de NTP.

Elemento o tarea de configuración	Especificación
Ajuste la fecha y hora en R2	Fecha actual
Configura R2 como un maestro NTP	R2(config)# R2(config)#ntp mas 48 R2(config)#ntp master 5 R2(config)#exit R2#%SYS-5-CONFIG_I: Configurad from console by console sh clock 9:8:19.289 UTC Sat MAR 5 2016
Configura R1 como un maestro NTP	R1(config)#ntp upda R1(config)#ntp update-calendar R1(config)#exit R1#%SYS-5-CONFIG_I:Configurad From console by console
Verifique la configuración de NTP en R1	R1#sh clock *5:49:38.876 UTC Mon Mar 1 1993 R1#shclock

Fuente. *Propia.*

A continuación, se observa la implementación de dichas instrucciones en CLI.

Figura 30 Instrucciones en CLI para la configuración de NTP.

```

User Access Verification

Password:

R1>enable
Password:
R1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#ntp server 172.16.1.2
R1(config)#ntp update-calendar
R1(config)#end
R1#
%SYS-5-CONFIG_I: Configured from console by console

R1#

```

Fuente. Propia.

2.7. Configuración y verificación de listas de control de acceso (ACL)

2.7.1. Paso 1: Restricción de acceso a las líneas vty en R2.

Para restringir el acceso a líneas vty en el router R2 se tiene:

Tabla 24 Listado de instrucciones para la configuración de restricción a líneas vty.

Elemento o tarea de configuración	Especificación
Configurar una lista de acceso con nombre para permitir que solo R1 establezca una conexión con R2	R2(config)#ipaccess-list standard ADMIN-MGT
Aplicar la ACL con nombres a las líneas vty	R2(config-std-nacl)#permit host R2(config-std-nacl)#permit host 172.16.1.1 R2(config-std-nacl)#deny an R2(config-std-nacl)#deny any 49 R2(config-std-nacl)#exi

Permitir acceso por Telnet a las líneas de vty	R2(config)#line vty 0 4 R2(config-line)#ipacc R2(config-line)#ipaccess-classa R2(config-line)#ip access-class ADMIN-MGT in R2(config-line)#trans R2(config-line)#transportin R2(config-line)#transport input te R2(config-line)#transport input telnet
Verificar que la ACL funcione como se espera	R1#telnet172.16.1.2Trying 172.16.1.2 ...OpenSe prohíbe el acceso no autorizado red JF User Access Verification Password: R2>exit [Connection to 172.16.1.2 closed By foreign host]

Fuente. *Propia.*

A continuación, se observa la implementación de dichas instrucciones en CLI.

Figura 31 Instrucciones en CLI para la restricción de acceso a líneas vty

```

R1#telnet 172.16.1.2
Trying 172.16.1.2 ...OpenSe prohíbe el acceso no autorizado

User Access Verification

Password:
R2>

```

Ctrl+F6 to exit CLI focus

4:53 a. m.
27/11/2021

Fuente. *Propia.*

2.7.2. Paso 2: Comandos en CLI.

Por último, se presenta una tabla con acciones posibles en CLI, en la columna derecha se debe complementar con el comando que ejecute dicha acción, con esto se tiene:

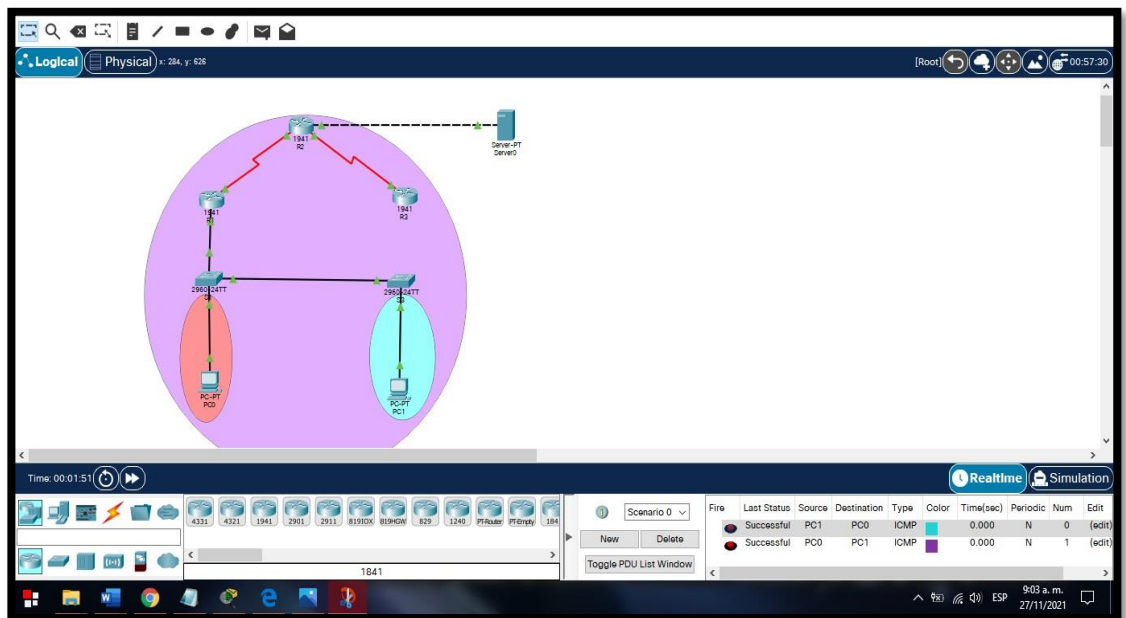
Tabla 25 Listado de comandos en CLI.

Descripción del comando	Comando
Mostrar las coincidencias recibidas por una lista de acceso desde la ultima vez que se restableció	R2#show access-lists Standard IP Access list 110 permit 192.168.21.0 0.0.0.255 (2 match(es)) 20 permit 192.168.23.0 0.0.0.255 30 permit 192.168.0.0 0.0.3.255 Standard IP access list ADMIN – MGT 10 permit host 172.16.1.1 20 deny any
Restablecer los contadores de una lista de acceso	R2#clear ip access – list counters
Que comando se usa para mostrar que ACL se aplica a una interfaz y la dirección en que se aplica?	R2#show ip interface GigabitEthernet0/0/0 is up, line protocol Is up (connected) Internet address is 209.165.200.233/29 Broadcast address Is 255.255.255.255
Con que comando se muestran las traducciones NAT?	R2#show ip nat translations Pro Inside Global Inside local Outside local Outside Global --- 209.165.200.233 10.10.10.10 --- --- tcp 209.165.200.225:1025 192.168.21.21:1025 209.165.200.238:80 209.165.200.238:80
Que comando se utiliza para eliminar las traducciones de NAT dinámicas.	Con el comando “clear ip nat translations all”

Fuente. Propia.

Ya con la red configurada a totalidad, el resultado final se observa en la figura 24.

Figura 32 Simulación final de la topología del segundo escenario.



Fuente. *Propia.*

Se observa en la parte inferior derecha que ambos computadores mediante un mensaje lograr conectarse, lo que nos indica que las configuraciones que se realizaron están funcionando correctamente.

CONCLUSIONES

Mediante el uso de la herramienta Packet Tracer en los múltiples ejemplos que se vieron, se detalla que a pesar de contar con una interfaz grafica para realizar la topología de redes y conexiones, es muy limitada frente a parámetros de configuración que se quieran establecer, por lo que si se desea explotar el máximo potencial de la herramienta es totalmente necesario el emplear y conocer en lo posible la mayoría de comandos y funciones de la terminal de comandos CLI de los dispositivos, pues con un buen uso de esta, no solo logramos ajustar parámetros o configuraciones de conexiones deseada, si no se puede llegar a establecer condiciones que ahorren recursos del sistema que de la forma con la interfaz grafica no se pueden llegar a configurar.

La revisión de las temáticas de las redes de área local y global permitió conocer, identificar y prevenir falencias o ataques a los que uno posiblemente puede llegar a estar expuesto, teniendo presente que si no se establecen correctamente parámetros de seguridad en la red uno esta susceptible a robo de información o suplantación, por lo cual siempre se debe ser consciente de programar y realizar una red de trabajo.

De igual manera, se comprendió que el uso de las VLAN puede constituirse como una llave mas de seguridad ya que al ser una red que es independiente dentro de otra física, se puede llegar a tratar de mejor manera la seguridad si se llegase a trabajar con computadores o dispositivos que estén compartiendo constantemente información.

Por último, el uso y estudio de protocolos como el protocolo OSPF permitió conocer que el envío de datos no siempre es igual, hay muchos factores que están implícitos en esto ya sea por el medio de transmisión, la carga que se trabaje o precisamente el protocolo que se emplee, donde algunos logran enviar la información más rápido pero puede llegar a perderse información,

como otros que son mas lentos pero la información se transmite de forma segura, por ello se debe tener en cuenta cuando se este diseñando una topología y hacia que ámbito estará destinada esta.

BIBLIOGRAFÍA

CCNA Desde Cero. (s.f.). Obtenido de
<https://ccnadesdecero.com/curso/ospf/>

CISCO. (2017). *Skills Assessment*.

Manage Engine. (2021). Obtenido de Configuración de NAT dinámico en dispositivos Cisco: <https://www.manageengine.com/latam/network-configuration-manager/configurar-nat-dinamico-dispositivos-cisco.html>

Mis libros de networking. (28 de 06 de 2015). Obtenido de
<http://librosnetworking.blogspot.com/2015/06/que-es-una-svi.html>

Romero Goyzueta, C. A. (s.f.). *Youtube*. Obtenido de Canal de Christian Augusto Romero Goyzueta II:
<https://www.youtube.com/channel/UC5P7maVk2idGTRB-himYf1w>